REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
01-06-2004	Bi-annual Performance/Technical Report	12/01/2003 - 05/31/2004

4. TITLE AND SUBTITLE

Bi-annual (12/2003--05/2004) Performance/Technical Report for ONR YIP Award under Grant N00014-03-1-0466
Energy Efficient Wireless Sensor Networks Using Fuzzy Logic

5a. CONTRACT NUMBER

5b. GRANT NUMBER

N00014 – 03 –1 –0466

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Liang, Qilian

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

University of Texas at Arlington
Office of Sponsored Projects
PO Box 19145
Arlington, TX 76019

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Office of Naval Research
800 North Quincy Street
Arlington, VA 22217-5660

10. SPONSOR/MONITOR'S ACRONYM(S)

ONR

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for Public Release; Distribution is Unlimited.

13. SUPPLEMENTARY NOTES

20040521 010

14. ABSTRACT

During the period of 12/1/2003 -- 5/31/2004, we have proposed different approaches on energy efficient wireless sensor networks. (1) We proposed a cross-layer design approach for fault-tolerance and energy efficiency. Network layer (sensor network routing), MAC layer, and physical layer (channel coding and interleaver) were considered in this approach. (2) Theory and performance analysis for sensor placement and lifetime of wireless sensor networks were studied, and statistical distribution of the node lifetime and network lifetime were presented. (3) A fully-distributed energy-efficient self-organizing protocol was proposed for wireless sensor networks, and an Expellant Self-Organization (ESO) scheme was developed. (4) Energy efficient intrusion detections and corresponding strategies were studied and simulated for wireless sensor networks. (5) Tradeoffs between latency and energy efficiency were evaluated in wireless sensor networks. Fourteen papers were produced during the past six months, and are attached to this report.

15. SUBJECT TERMS

Wireless Sensor Network, Energy Efficiency, Fuzzy Logic, Fault-Tolerant, Security.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Qilian Liang
U	U	U	UU	139	19b. TELEPHONE NUMBER *(Include area code)* 817-272-1339

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

Bi-annual (12/2003–05/2004) Performance/Technical Report for ONR YIP Award under Grant N00014-03-1-0466 Energy Efficient Wireless Sensor Networks Using Fuzzy Logic

Qilian Liang
Department of Electrical Engineering
University of Texas at Arlington
Arlington, TX 76019-0016 USA
Phone: 817-272-1339, Fax: 817-272-2253
E-mail: liang@uta.edu

Abstract

During the period of 12/1/2003 – 5/31/2004, we have proposed different approaches on energy efficient wireless sensor networks.

1. We proposed a cross-layer design approach for fault-tolerance and energy efficiency. Network layer (sensor network routing), MAC layer, and physical layer (channel coding and interleaver) were considered in this approach.
2. Theory and performance analysis for sensor placement and lifetime of wireless sensor networks were studied, and statistical distribution of the node lifetime and network lifetime were presented.
3. A fully-distributed energy-efficient self-organizing protocol was proposed for wireless sensor networks, and an Expellant Self-Organization (ESO) scheme was developed.
4. Energy efficient intrusion detections and corresponding strategies were studied and simulated for wireless sensor networks.
5. Tradeoffs between latency and energy efficiency were evaluated in wireless sensor networks.

Fourteen papers were produced during the past six months, and are attached to this report.

1 Fault-tolerant and Energy Efficient Cross-Layer Design for Wireless Sensor Networks

In wireless sensor networks, fault-tolerance and energy efficiency are two important topics. We studied fault-tolerance for link failure and compromised nodes (because of security attacks) using a cross-layer approach: considering network layer (sensor network routing), MAC layer, and physical

layer (channel coding and interleaver). Energy efficiency was also considered in the cross-layer approach.

1.1 Energy and Mobility Aware Geographical Multipath Routing for Wireless Sensor Networks

In [4], we proposed a fully-distributed energy and mobility aware geographical multipath routing for wireless sensor networks. The remaining battery capacity, mobility, and distance to the destination location of candidate sensors in the local communication range were taken into consideration for next hop relay node selection, and a fuzzy logic system was applied to the decision making. Simulation results showed that this scheme could extend the network lifetime longer than the original geographical routing scheme which only considers distance to the destination location, and this scheme could reduce the frame loss rate and link failure rate since mobility was considered.

1.2 Fault Tolerant Multipath Transportation Aided with Channel Coding and Interleaver

In wireless sensor networks, the bandwidth and energy are limited, and some link failures may happen during data transmission. In [1][2], we proposed a fault tolerant Multipath Transportation Aided with Channel Coding and Interleaver (MTACCI) scheme for Wireless Sensor Networks. We drew the following conclusions:

1. Simulation results showed that our scheme performed much better than the Dual Transportation (DT) scheme (in static AWGN channel) and diversity with MRC scheme (in fading channel) in terms of BER.

2. Our MTACCI could tolerate some link failures, which makes wireless sensor networks survivable and resilient.

3. Our MTACCI scheme needs much narrower bandwidth than the other two schemes, which solves the bandwidth constraint problem in wireless sensor networks.

4. Our MTACCI scheme can work at low SNR, which can save lots of energy because energy constraint is one of the most important topics in wireless sensor networks, and existing studies showed that most energy is consumed in communication-related activies in wireless sensor networks.

5. The larger the number of paths in MTACCI, the better the performance, which means the fault is more tolerable. In additions, the required bandwidth is narrower for larger number of paths in MTACCI.

1.3 Secure and Energy Efficient Multipath-routing (SEEM) in Wireless Sensor Networks: A Cross-Layer Approach

In wireless sensor networks, security and energy efficiency are two important topics. In multipath routing, threat can come from compromised nodes, which might relay incorrect information (packet) to the next node during routing. Detection of such incorrect information is very difficult. In [3][2], we proposed a Secure and Energy Efficient Multipath-routing (SEEM) scheme aided with channel coding and interleaver. The M-path in multipath routing were selected using existing routing algorithm and fuzzy logic system considering the average remaining battery capacity and mobility of associated nodes. Simulation results showed that even if certain paths were compromised, the receiver node was still able to recover the transmitted message from errors with very low bit error rate.

2 Sensor Placement and Lifetime of Wireless Sensor Networks: Theory and Performance Analysis

The energy constraint on wireless sensor networks leads to limited lifetime. Architects of such networks are required to guarantee a specific network lifetime for specific applications. In [6][7], we proposed an analytical network lifetime evaluation methodology that can be used to arrive at a closed form expression for network lifetime. This methodology is easy to follow. Also, its bottom-up nature, which views the problem at the sensor node level instead of network level, makes the approach simpler and faster. As a first step towards validating this approach, we applied it to networks having regular sensor placement schemes. The schemes chosen for evaluation were the square grid and the hex grid placement schemes where the sensor nodes are placed at the corners of squares and regular hexagons respectively. We assumed the square grid networks and the hex grid networks to be deployed with least density, i.e., distance between adjacent nodes is equal to the sensing/communication range of an individual sensor. All sensor nodes were assumed to be identical. Lifetime was defined as the post deployment time interval for which the network maintains complete coverage and connectivity. The analytical approach that we proposed has the following three steps:

1. Failure analysis
2. Node lifetime evaluation
3. Network lifetime evaluation.

The first step analyzes the reasons for network failure. The failure analysis of the two grids shows that the two main reasons for network failure are loss of coverage and loss of connectivity, and this occurs when any two neighboring nodes fail. High-density networks (distance between adjacent

nodes is ¡ sensor range) are also analyzed for network failure. The second step evaluates the sensor node lifetime. The lifetime of a sensor node is defined as the time taken for its energy to go zero. It is modeled as a random variable, and its reciprocal is found to follow a Gaussian distribution. The third step, which is the network lifetime evaluation, requires the application of reliability theory. Reliability block diagrams are built to model network failure. Survivor functions of node lifetimes are used to find the network lifetime survivor function, and hence the probability distribution of the network lifetime. Simulation results and theoretical plots show strong similarities. Lifetime evaluation is high-density networks uses the corresponding least density network lifetime, as well as the node survivor function to evaluate the time taken for the high-density network to reach the least-density state. The analysis performed on 36-node square grids and hex grids showed that although the hex grids covers almost double the area as compared to the square grid, it delivers the same lifetime. Comparisons such as this can enable sensor network architects decide which placement pattern best suits the application. This methodology can also be used to choose between several possible routing protocols or data aggregation schemes, based on the lifetime that they deliver. The square grid and the hex-grid are basic four-neighbor and three-neighbor placement schemes and can be used as basis for evaluation of other complex placement schemes. The analysis can also be extended to randomly deployed networks.

3 Energy-Efficient Self-Organization for Wireless Sensor Networks: A Fully Distributed Approach

Clustering provides a promising hierarchy in energy efficiency. In [12], we first adapted Low-Energy Adaptive Clustering Hierarchy (LEACH) to more dynamic topologies which is associated with sensor networks. By relying the clustering on the one-hop neighbor information, we removed LEACH's dependence on other routing schemes. Furthermore, we introduced adaptive channel assignment to accommodate the on-off topology changes. However, we noticed that the optimal number of clusters obtained through simulations does not agree with the analysis. Through extensive study, we found this is mainly due to the random head election used in LEACH can not guarantee the desired number of clusters be elected, which shifts the outcome of election to a larger number of clusters (see [13, 14] for details). To address this problem, in [13, 14], we proposed using cluster radius to replace the number of clusters as the guideline parameters. Nevertheless, we developed Expellant Self-Organization (ESO) scheme to guide the election. ESO makes good use of the contention for wireless medium to choose the strongest node to be the cluster head so that not only the approximately desire number of clusterheads be elected but also they are evenly distributed in the whole network. Thanks to better outcome of head election, ESO achieves energy efficiency comparable with LEACH in terms of network life and Data/Energy Ratio without involving global information in clustering.

4 An Energy-Efficient Self-Organizing Protocol for Wireless Sensor Networks

In [5], we consider a network of energy-constrained sensors deployed over a region. Each sensor node in such a network is systematically gathering and transmission sensed data to a base station (via clusterhead) for further processing. A key challenge in data gathering is to maximize the system lifetime, given the energy constraints. We focused on reducing the power consumption of wireless sensor networks. The dominate component in energy consumption is almost always due to communication. Therefore, we heavily modified an existing communication protocol, Low-Energy Adaptive Clustering Hierarchy (LEACH). We extend LEACH's stochastic cluster-head selection algorithm by a deterministic component to reduce energy consumption. Simulation results showed that our modified scheme can extend the network life around 50% for First Node Dies (FND) and 62% for Last Nodes Dies (LND).

5 Energy Efficient Intrusion Detections and Strategies for Wireless Sensor Networks

Denial of Service(DoS) attack on Wireless Sensor Networks(WSN) might attempt to disrupt/degrade the function of the whole network or might harm a specific node. This type of attack is critical in any security system. Without proper security mechanisms, networks will be confined to limited, controlled environments, negating much of promise they hold. While DoS has been studied extensively for the wire-line networks, it is lack enough of research in WSN. Due to deployment in tactical battlefield missions, WSN is susceptible to attacks by malicious intruders. Meanwhile, some salient features of WSN lay challenges in securing the security of message transmitted in the networks. DoS attack on MAC layer of WSN could potentially disrupt channel access and might cause waste of bandwidth and power resources. When some normal nodes were captured and reprogrammed by enemies, traditional security mechanisms, such as authentication protocols, digital signature, and encryption, are not strong enough to make WSN be immune for all kinds of attacks. Through adding our algorithm to the RTS/CTS based MAC protocols, we improved the safety of MAC layer.

In [8][9], we proposed a security algorithm which has two function modules for it: intrusion detection module and intrusion defense module. The basic idea behind the algorithm is that, intrusion module of each node frequently monitors a serial of sensitive network performance indicators, then according to these statistics' values, the intrusion module make the decision, i.e. whether the intrusion existed or not. If intrusion is found, the defense module of each node schedules the countermeasure to reduce the destroy of the attacker. After a period of time, the node would make intrusion detection again. We especially studied Collision attack, Unfairness attach and Exhaustion attack. We applied soft decision theory [8] and fuzzy logic theory [9] separately to carry out our

intrusion detection task. In soft decision approach [8], we made intrusion detection based on the values of Collision Ratio(R_c), Probability of Data Packet Successful Transmission(P_{st}), Data Packet's Waiting-Time(T_w) and RTS Packets Arrival Ratio(R_{RTS}). This is a soft decision approach. The advantage of using soft decision is that we can effectively reduce the chance to make fault decision, which is caused by very small fluctuation of any indicator's value. In fuzzy logic decision approach [9], we detected the intrusion using the values of R_c(x1), T_w(x2) and R_{RTS}(x3). We found that it is a waste of energy or unsafe action for the node to try to transmitting or receiving information during intrusion period. The reason is, the transmitting or receiving is almost unsuccessful or spied by attackers when enemies attack the network. Besides, there is no center control station in the network, and we don't hope to utilize the cooperation among nodes. For energy efficiency purpose, stopping transmitting and receiving at this time is a feasible method to avoid the intrusion. Our countermeasure is to force the node switch to sleep mode for a period of time, when it finds the intrusion happen. And each node schedules its sleep plan individually.

Simulation results showed that our detection algorithm could detect all collision attack, exhaustion attack and unfairness attack successfully when intrusion happened. At the same time, the false alarm rate is 0. Furthermore, our defense algorithm scheduled protection plans successfully. For our approach, the function modules are executed by each node separately and automatically. Co-operations among nodes are not required. Therefore it is a distributed method. In addition, no extra hardware is needed.

6 Latency and Energy Efficiency Aware Wireless Sensor Networks

Performance evaluation was one of the most important research topics for the Wireless Sensor Networks (WSN). Latency-aware and energy efficiency were two important parameters to evaluate the networks quality. In order to meet different performance requirements of the service, we classified the packets into high priority and low priority. In [10][11], we considered the latency and energy tradeoffs in WSN. The latency of the high priority packets was small but the network cost more energy. The latency of the packets of low priority packets was large but the network cost less energy. We solved this problem by transmitting redundant packets in the WSN. We assumed that the network had a cell-partitioned structure, and sensor moved according to one-step Markov path model with constant speed. The power consumption ratio: Transmit: receive: idle of the sensor node was approximately: 40:20:1. Each sensor could generate packets with a Poisson distribution and each sensor could reserve original packets and relay packets. Each packet entered its subqueue according to its destination node ID. The 2-Hop relay algorithm was introduced in the networks. This relay algorithm restricted packets to 2-hop paths, and the relay packet was inserted into the subqueue of the relay sensors until a source encountered its destination. We implemented the simulation model using the OPNET modeler. Simulation showed that the scheduling algorithm with/without redundancy could realize the latency/energy tradeoffs in WSN. The contributions were twofold:

first, we classified the sensor service into two priorities: high and low. The higher priority, the better delay performance and more energy consumption. We realized it with the two-hop relay algorithm. Second, we established energy/delay tradeoffs curve for the performance of the two-hop relay algorithm.

In order to improve the performance of the two-hop relay algorithm, in [11], the Fuzzy logic system (FLS) was implicated in the sensor nodes selection. We modified the network model with a cell-partitioned structure: sensor moves according to one-step Markov path model with variable speed and the distance between two nodes were variable in the WSN and the power loss model was used. FLS was used to elect the three relay nodes. When there were several pairs within one cell, we used the FLS to elect the destination node. Three descriptors were used: distance to the source node, the remaining energy and the degree of mobility. The output of FLS application provides a node election probability and we could elect three highest probability nodes as the relay nodes and in another FLS application, we chose the highest probability node as the destination. In contrast with the cases that only considered one descriptor, simulation results showed that the FLS application could manage the delay/energy tradeoffs. If we design different FLS in the two-hop relay algorithm, we can meet different performance requirement in WSN.

References

[1] Qilian Liang, Lingming Wang, "Fault-Tolerant Multipath Transportation Aided with Channel Coding and Interleaver for Wireless Sensor Networks," accepted by *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Sept 2004, Barcelona, Spain.

[2] Qilian Liang, Lingming Wang, "Fault-tolerant and Energy Efficient Cross-Layer Design for Wireless Sensor Networks," submitted to *IEEE Transactions on Mobile Computing.*

[3] Qilian Liang, Lingming Wang, "Secure and Energy Efficient Multipath-routing (SEEM) in Wireless Sensor Networks: A Cross Layer Approach," submitted to *IEEE Globecom*, Nov 2004, Dallas, TX.

[4] Qilian Liang, Qingchun Ren, "Energy and Mobility Aware Geographical Multipath Routing for Wireless Sensor Networks," submitted to *IEEE MILCOM*, Oct 2004, Montery, CA.

[5] Hsiao-Lan Hsu, Qilian Liang, "An energy efficient protocol for wireless sensor networks," accepted by *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Sept 2004, Barcelona, Spain.

[6] Ekta Jain, Qilian Liang, "Sensor Placement and Lifetime of Wireless Sensor Networks: Theory and Performance Analysis," submitted to *IEEE Transactions on Mobile Computing.*

[7] Ekta Jain, Qilian Liang, "Sensor Placement and Lifetime of Wireless Sensor Networks: Theory and Performance Analysis," submitted to *IEEE Globecom*, Nov 2004, Dallas, TX.

[8] Qingchun Ren, Qilian Liang, "Secure Media Access Control (MAC) in Wireless Sensor Networks: Intrusion Detections and Countermeasures," accepted by *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Sept 2004, Barcelona, Spain.

[9] Qingchun Ren, Qilian Liang, "Secure Media Access Control in Wireless Sensor Networks: Intrusion Detections and Strategies," submitted to *IEEE MILCOM*, Oct 2004, Montery, CA.

[10] Xinsheng Xia, Qilian Liang, "Latency Aware and Energy Efficiency Tradeoffs for Wireless Sensor Networks," accepted by *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Sept 2004, Barcelona, Spain.

[11] Xinsheng Xia, Qilian Liang, "Latency and Energy Efficiency Evaluation in Wireless Sensor Networks," submitted to *IEEE MILCOM*, Oct 2004, Montery, CA.

[12] Liang Zhao, Qilian Liang, "Distributed and energy efficient self-organization for on-off wireless sensor networks," accepted by *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Sept 2004, Barcelona, Spain.

[13] Liang Zhao, Xiang Hong, Qilian Liang, "Energy-Efficient Self-Organization for Wireless Sensor Networks: A Fully Distributed Approach," submitted to *IEEE Transactions on Wireless Communications*.

[14] Liang Zhao, Xiang Hong, Qilian Liang, "Energy-Efficient Self-Organization for Wireless Sensor Networks: A Fully Distributed Approach," submitted to *IEEE Globecom*, Nov 2004, Dallas, TX.

Fault-Tolerant Multipath Transportation Aided with Channel Coding and Interleaver for Wireless Sensor Networks

Qilian Liang and Lingming Wang
Department of Electrical Engineering
University of Texas at Arlington
Arlington, TX 76019-0016 USA
E-mail: liang@uta.edu, wang@wcn.uta.edu

Abstract— **In wireless sensor networks, the bandwidth and energy are limited, and some link failures may happen during data transmission. In this paper, we propose a fault tolerant Multipath Transportation Aided with Channel Coding and Interleaver (MTACCI) scheme for Wireless Sensor Networks. Simulation results show that this scheme works much better than the dual transportation scheme in static channel and diversity combining scheme in fading channel when link failures exist. Further analysis demonstrates that this scheme can solve the bandwidth and energy constraint problems, and makes wireless sensor networks survivable and resilient.**

Index Terms : Wireless sensor networks, multipath transportation, fault tolerant, channel coding, channel fading.

I. Introduction

Wireless sensor networking is an emerging technology that promises unprecedented ability to monitor and manipulate the physical world via a network of densely distributed wireless sensor nodes. The nodes can sense the physical environment in a variety of modalities, including acoustic, seismic, thermal, and infrared. The data rate can vary significantly between different types of sensors. For example, the temperature sensor works at a frequency significantly less than 1 Hz and generates less than one byte of information at one time, while a high resolution video camera can generate 10's of megabits of information per second. In wireless sensor networks, there exists some challenges:

- Bandwidth is limited, which raises some challenges in information and data transportation in wireless sensor networks, especially in sensor networks for video services, which involves a large amount of data.
- The routing path (link) failure may happen during data transmission because of collision, node dying out (no battery), node busy, or other accidents.
- There exists energy constraint in wireless sensor networks because most sensors are battery operated, which means the operating signal-to-noise-ratio (SNR) is very low.
- Some applications require real time information and data, which means re-transmission is not possible.

These challenges motivate us to design a fault-tolerant transportation scheme for wireless sensor networks. In this paper, we propose a fault-tolerant multipath transportation scheme aided with channel coding and interleaver in wireless sensor networks.

The idea of utilizing path diversity in multimedia data transmission was proposed in [6], which mainly considered image transmission. Recently, Lin *et al* [12] presented a reference picture selection scheme based on feedback for video transmission over multiple paths. Layered coding combined with a selective Automatic Repeat reQuest (ARQ) transport scheme was proposed in [13], in which base layer and enhancement layers are transmitted over different paths and only base layer is allowed to be retransmitted. Both schemes are under the assumption that the channel is feedback channel. Aramvith *et al* [1] proposed a conditional retransmission strategy to reduce the number of retransmissions so that to improve the video quality for wireless video.

In Section II, we introduce some preliminary knowledges on channel fading. In Section III, we present our Multipath Transportation Aided with Channel Coding and Interleaver (MTACCI) Scheme. The simulation results and performance analysis are presented in Section IV, and in Section V, we conclude this paper.

II. Preliminary Knowledge on Channel Fading

In mobile wireless sensor networks, some sensors are mobile, which will have channel fading during data transportation. We model such fading as Rician fading. Rician fading occurs when there is a strong specular (direct path or line of sight component) signal in addition to the scatter

(multipath) components. The channel gain,

$$g(t) = g_I(t) + jg_Q(t) \quad (1)$$

can be treated as a wide-sense stationary complex Gaussian random process, and $g_I(t)$ and $g_Q(t)$ are Gaussian random processes with non-zero means $m_I(t)$ and $m_Q(t)$, respectively; and they have same variance σ_g^2, then the magnitude of the received complex envelop has a Rician distribution,

$$p_\alpha(x) = \frac{x}{\sigma^2}\exp\{-\frac{x^2+s^2}{2\sigma^2}\}I_0(\frac{xs}{\sigma^2}) \quad x \geq 0 \quad (2)$$

where

$$s^2 = m_I^2(t) + m_Q^2(t) \quad (3)$$

and $I_0(\cdot)$ is the zero order modified Bessel function. This kind of channel is known as Rician fading channel. A Rician channel is characterized by two parameters, Rician factor K which is the ratio of the direct path power to that of the multipath, i.e., $K = s^2/2\sigma^2$, and the Doppler spread (or single-sided fading bandwidth) f_d. We simulate the Rician fading using a direct path added by a Rayleigh fading generator. The Rayleigh fade generator is based on Jakes' model [8] in which an ensemble of sinusoidal waveforms are added together to simulate the coherent sum of scattered rays with Doppler spread f_d arriving from different directions to the receiver. The amplitude of the Rayleigh fade generator is controlled by the Rician factor K. The number of oscillators to simulate the Rayleigh fading is 60.

III. Multipath Transportation Aided with Channel Coding and Interleaver Scheme

In our scheme, the multipaths to be used for transportation can be be chosen using routing. Many routing protocols have been developed for ad hoc sensor networks, which can be summarized as two categories: table-driven (e.g., destination sequenced distance vector [2], cluster switch gateway routing [4]) and source-initiated on-demand-driven (e.g., ad hoc on-demand distance vector routing [15], dynamic source routing [9]). In [10], Lee and Gerla proposed a Split Multipath Routing protocol that builds maximal disjoint paths, where data traffic is distributed in two roots per session to avoid congestion and to use network resources efficiently. A Multipath Source Routing (MSR) scheme was proposed in [19], which is an extension of Dynamic Source Routing (DSR). Their work focuses on distributing load adaptively among several paths. Nasipuri and Das [14] presented the On-Demand Multipath Routing scheme, which is also an extension of DSR. In their scheme, alternative routes are maintained, which can be utilized when the primary one fails. Tsirigos and Haas [18] proposed a multipath routing scheme based on Diversity Coding. Three different paths are utilized to distribute the data, and x-for-y Diversity Coding is used to offer protection against at most x lost blocks out of the total $x + y$ blocks.

The number of paths (M-path) to be used for transportation is determined based on the channel bandwidth and symbol rate. Based on Shannon channel capacity formula [16],

$$C = W\log(1 + SNR) \quad (4)$$

where C is the channel capacity in $bits/sec$; $W(Hz)$ is the channel bandwidth; and SNR is the signal-to-noise ratio. The transmitted bit rate $Ibits/sec$ has to satisfy $I < C$ theoretically. For very limited bandwidth per channel in wireless sensor networks, C will not be very high. In additions, it is very desirable if there is no intersymbol interference (ISI) so that the sensor networks can work at very low SNR to save energy and extend the network lifetime. To ensure there is no ISI, the symbol rate $Rsym/sec$ (in transmission) has to be less than the channel bandwidth (WHz). Suppose the channel bandwidth is WHz, and symbol rate is $Vsym/sec$, then M (number of paths) can be approximately chosen as a minimum integer which satisfies $M \geq V/W$. Existing routing scheme provides some candidate paths. How to choose M paths from given candidates will be discussed in another paper. In this paper, we assume M paths have been chosen. During the multipath transportation, some fault (failure) modes may occur because of collision, node dying out (no battery), node busy, or other accidents.

In this paper, we propose a multipath transportation aided with channel coding and interleaver (MTACCI) scheme. We apply convolutional coding to encode the information bits, then the code words are interleaved. Interleaver [20] was used to eliminate the correlation of the noise/fading process affecting adjacent symbols in a received code word, but here we use interleaver to make sure that the lost symbols in one failure path will be spreaded after de-interleaver so that the Viterbi decoder will perform well. The interleaved bits are inserted with some unique words (for demodulation purpose), and then these bits are modulated to symbols. By this means, a frame has been built. For M-path transportation, we split the symbols in one frame to M equal-length bursts, and each path transmits one burst in parallel. The receiver node demodulates each successfully received burst from different path and provide soft-decision output. The receiver node combines all the soft-decision output from each burst according to the order when they are transmitted, and in case one or more bursts are lost due to link failure during transmission, the receiver node will provide 0's as the soft decision output. In this paper, we use the demodulation algorithm we proposed in [11] for soft decision output. De-interleaving is performed to the soft-decision output, and the de-interleaved data are used as the input to Viterbi decoder. The decoded output from Viterbi decoder are the

information bits with possible errors due to link failure and additive white Gaussian noise (AWGN). We summarize this scheme using a diagram in Fig. 1.

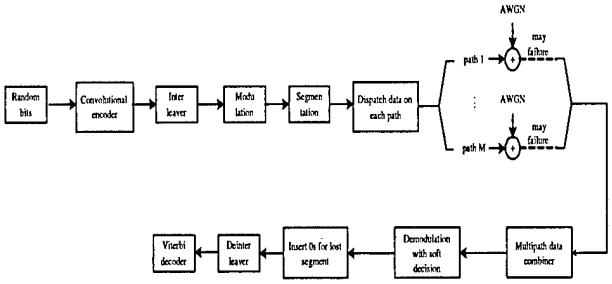


Fig. 1. The diagram of MTACCI.

IV. Simulations and Performance Analysis

We evaluated our MTACCI scheme using computer simulations. We ran our simulations for four-path transportation (Experiment I) and six-path transportation (Experiment II), and assumed each path has 2% failure rate. QPSK modulation and convolutional codes with rate $\frac{1}{2}$ and connections 101 and 111 (in binary) were used in the transmitting sensor (encoder) and receiver node (Viterbi decoder).

A. Four-Path MTACCI

In Experiment I, the information bit rate requires $1.6Mb/sec$, but the channel bandwidth is only $533KHz$, and roll-off factor for square-root raised cosine filter is 0.3. To avoid ISI, we used four-path transportation. The frame structure is plotted in Fig. 2 (a) with 820 QPSK symbols (800 symbols payload and 20 symbols UW) were used. We used block interleaver with size 8×200 to interleave the payload bits (after channel coding), and then then construct a frame by inserting UW and modulation. One frame is splitted to four equal-length bursts ($205sym/burst$) for transmission, and transmitting such a burst needs $0.5ms$, which means symbol rate per channel is $410Ksym/sec$, so it guarantees that there is no ISI during transmission (considering the roll-off factor 0.3 already). The total information bit rate in the four-path is $1.6Mb/sec$ (considered channel coding rate $\frac{1}{2}$ and QPSK modulation), which satisfies the requirement.

We ran Monte-Carlo Simulations for 10^5 frames at each E_b/N_0 value, and compared its performance against conventional dual transportation (DT) [5]. In dual (2-path) transportation, the transmitted symbols in each path are identical, but it will have big advantage if one path has failure during transportation. In the simulation, the frame in each path has 400 payload symbols and 10 UW symbol per burst without coding (illustrated in Fig. 2(b)). Considering two paths, the total number of symbols (820 symbols) is the same as the MATCCI per transportation. But to achieve information bit rate $1.6Mb/sec$, transmitting such a frame needs $0.5ms$, which means the symbol rate is $820Ksym/sec$. A wider bandwidth at least $1.066MHz$ (considering the roll-off facot 0.3) is required for this scheme. We provided such bandwidth to DT scheme and compared with our four-path MTACCI scheme (with $533KHz$ per channel). In Fig. 3, we summarized the average bit error rate (BER) versus E_b/N_0. Observe that the MTACCI scheme has more than 3dB gain comparing to the DT scheme. It clearly shows a BER floor for the MTACCI scheme at high E_b/N_0 because there exists 2% failure rate for each path. But the performance of our MTACCI is very good (e.g., $BER = 3 \times 10^{-4}$ at $E_b/N_0 = 5dB$). In additions, the MTACCI scheme needs only half bandwidth ($533KHz$) as that required by the DT scheme ($1.066MHz$).

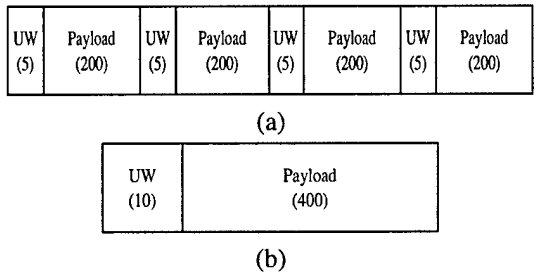


Fig. 2. Frame structure (in symbols) we used in our simulations. (a) Six-path MTACCI, (b) Dual transportation or diversity with MRC.

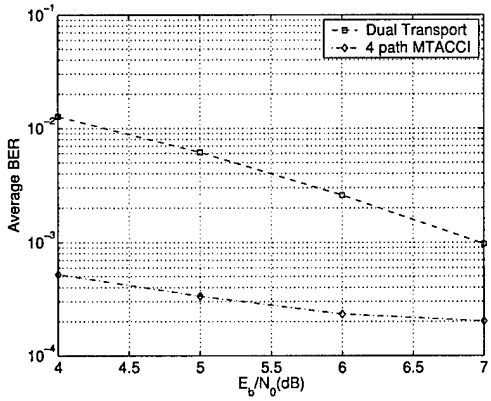


Fig. 3. Average BER versus E_b/N_0 for four-path MTACCI and dual transportation (DT) in static AWGN channel.

In mobile wireless sensor networks, there exists channel fading during data transportation. In the simulation, we used Rician fading $K = 9dB$ and $f_d = 20Hz$. We compared our MTACCI scheme against the two-path diversity with maximal ratio combination (MRC) scheme. Diversity

is very powerful in combatting channel fading [17], and MRC is the optimal combination scheme for diversity. We used the same frame structure as that in dual transportation scheme (Fig. 2b). We ran Monte-Carlo Simulations for 2×10^5 frames at each E_b/N_0 value for four-path MTACCI and diversity with MRC, and summarized the results in Fig. 4. Observe that four-path MTACCI can achieve more than $1dB$ gain at $BER = 10^{-3}$.

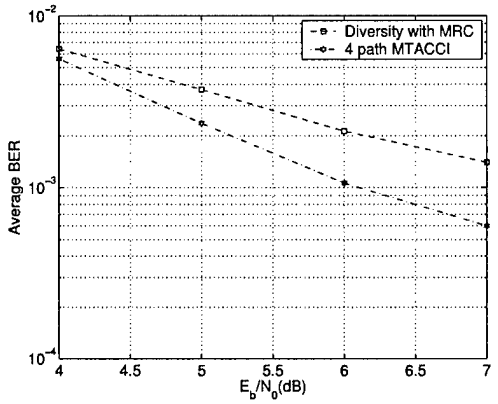


Fig. 4. Average BER versus E_b/N_0 for four-path MTACCI and diversity with MRC in Rician fading channel ($K = 9dB$, $f_d = 20Hz$).

In addition to the gains in terms of dB of E_b/N_0, the MTACCI scheme needs only half bandwidth ($533KHz$) compared to the diversity with MRC ($1.066MHz$).

B. Six-Path MTACCI

In Experiment II, the information bit rate requires $1.6Mb/sec$ (same as that in Experiment I), but the channel bandwidth is only $347KHz$, and roll-off factor for square-root raised cosine filter is 0.3. To avoid ISI, we used six-path transportation. The frame structure is plotted in Fig. 5 (a) with 930 QPSK symbols (900 symbols payload and 30 symbols UW) were used. We used block interleaver with size 12×150 to interleave the payload bits (after channel coding), and then then construct a frame by inserting UW and modulation. One frame is splitted to six equal-length bursts ($155sym/burst$) for transmission, and transmitting such a burst needs $0.56ms$, which means symbol rate per channel is $276.8Ksym/sec$, so it will ensure that there is no ISI during transmission given that channel bandwidth is $347KHz$ and roll-off factor is 0.3. The total information bit rate in the six-path is $1.6Mb/sec$ (considering channel coding rate $\frac{1}{2}$ and QPSK modulation), which satisfies the requirement.

We ran Monte-Carlo Simulations for 10^5 frames at each E_b/N_0 value, and compared its performance against the DT scheme. The frame structure is provided in Fig. 5(b). Very similar analysis as in Section IV-A, we can draw a conclusion that the DT scheme needs a bandwidth at least

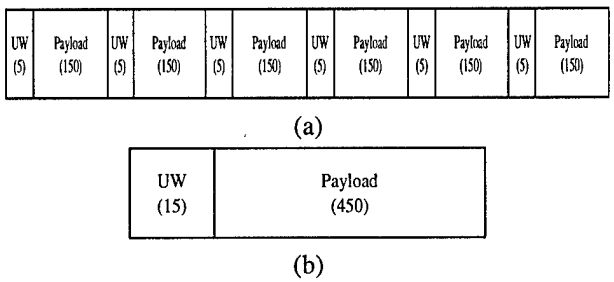


Fig. 5. Frame structure (in symbols) we used in our simulations. (a) Six-path MTACCI, (b) Dual transportation or diversity with MRC.

$1.041MHz$. In Fig. 6, we plotted the average BER versus E_b/N_0 for these two schemes. Observe that more than 4 dB gain can be achieved using MTACCI.

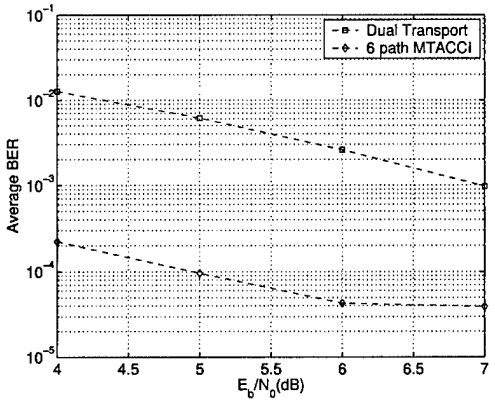


Fig. 6. Average BER versus E_b/N_0 for four-path MTACCI and dual transportation (DT) in static AWGN channel.

Similarly to Section IV-A, we performed simulations for Rician fading channel $K = 9dB$ and $f_d = 20Hz$, and compared our six-path MTACCI against the two-path diversity with MRC. The simulation results are summarized in 7, which demonstrates that more than 2 dB gain can be achieved using six-path MTACCI.

Again, we re-iterate the bandwidth efficiency of our six-path MTACCI: $347KHz$ versus $1.041MHz$ (for DT or diversity with MRC).

Observe Figs. 3 and 6, and Figs. 4 and 7, for larger number of paths in MTACCI, the performance is better, which means the fault is more tolerable. In additions, the required bandwidth is narrower for larger number of paths in MTACCI.

C. Why Fault Can be Tolerated?

Why our MTACCI scheme can perform very well even with high failure rate (2%) in each path? This can be explained based on the successful example of puncturing. Puncturing is often used to generate additional rates from

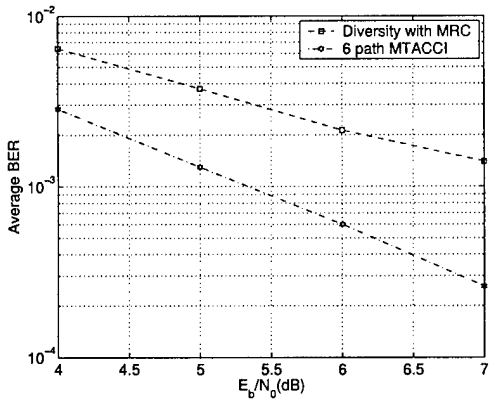


Fig. 7. Average BER versus E_b/N_0 for six-path MTACCI and diversity with MRC in Rician fading channel ($K = 9dB$, $f_d = 20Hz$).

a single convolutional code [3][7]. The basic idea behind puncturing is not to transmit some of the bits output by the convolutional encoder, thus increase the rate of the code. This increase in rate decrease the free distance of the code, but usually the resulting free distance is very close to the optimum one. The receiver inserts dummy bits to replace the punctured bits in the receiver, hence only one encoder/decoder pair is needed to generate several different code rates. In our M-path routing, the receiver node will insert 0's if one burst is lost during transmission, and then de-interleave these soft-decision output from demodulator, which is very similar to puncturing. But in our scheme, the effective puncturing pattern in terms of the number of bits and puncture location is time-varying from frame to frame.

V. Conclusions

We have proposed a fault-tolerant MTACCI scheme for wireless sensor networks.

1) Simulation results show that our scheme performs much better than the DT scheme (in static AWGN channel) and diversity with MRC scheme (in fading channel) in terms of BER.
2) Our MTACCI can tolerate some link failures, which makes wireless sensor networks survivable and resilient.
3) Our MTACCI scheme needs much narrower bandwidth than the other two schemes, which solves the bandwidth constraint problem in wireless sensor networks.
4) Our MTACCI scheme can work at low SNR, which can save lots of energy because energy constraint is one of the most important topics in wireless sensor networks, and existing studies show that most energy is consumed in communication-related activies in wireless sensor networks.
5) The larger the number of paths in MTACCI, the better the performance, which means the fault is more tolerable. In additions, the required bandwidth is narrower for larger number of paths in MTACCI.

Acknowledgement

This work was supported by the U.S. Office of Naval Research (ONR) Young Investigator Program Award under Grant N00014-03-1-0466.

References

[1] S. Aramvith, C.W. Lin, S. Roy, and M.T. Sun " Wireless Video Transport Using Conditional Retransmission and Low-Delay Interleave ," *IEEE Tans. Circuit Systm. Video Technol.*, vol. 12, pp. 558-565, Jun. 2002

[2] C. P. Bhagwat, "Highly dynamic destination-sequenced distance vector routing," *Proc. of ACM SIGCOMM'94*, pp.234-244, Sept 1994.

[3] J. B. Cain, G. C. Clark Jr, and J. M. Geist, "Punctured convolutional codes of rate (n-1)/n and simplified maximum likelihood decoding," *IEEE Trans on Information Theory*, vol. 25, pp. 97-100, Jan 1979.

[4] C. -C. Chiang, et al, "Routing in clustered multihop mobile wireless networks with fading channel," *Proc. IEEE Singapore Intl Conference on Networks*, 1997.

[5] S. Dulman, et al, "Trade-off between traffic overhead and reliability in multipath routing for wireless sensor networks," *IEEE WCNC*, March 2003, New Orleans.

[6] N. Gogate, and S.S. Panwar, " Supporting video/image applications in a mobile multihop radio enviroment using route diversity ," *Proceedings of ICC.* , Jun. 1999.

[7] J. Hagenauer "Rate compatible punctured convolutional codes and their applications," *IEEE Trans on Communications*, vol. 36, pp. 389-400, April 1988.

[8] W. C. Jakes, *Microwave Mobile Communication*, New York, NY: IEEE Press, 1993.

[9] D. Johnson and D. Maltz, *Mobile Computing*, Kluwer Academic Publishers, 1996.

[10] S.J. Lee, and M. Gerla, " Split Multipath Routing with Maximally Disjoint Paths in Ad Hoc Networks ," *ICC 2001.*,

[11] Q. Liang, "Optimal demodulator for satellite-based wireless ATM networks," *IEEE International Conference on Communications (ICC)*, May 2003, Alaska.

[12] S. Lin, S. Mao, Y. Wang, and S. Panwar, " A Reference Picture Selection Scheme for Video Transmission over Ad-hoc Networks Using Multiple Paths ," *Proceedings of ICME.* , Aug. 2001,

[13] S. Mao, S. Lin, Y. Wang, and S. Panwar " Reliable Transmissions of Video over Ad-hoc Networks Using Automatic Repeat Request and Multi-path Transport ," *Proceedings of VTC* , Oct. 2001

[14] A. Nasipuri, and S.R. Das, " On-Demand Multipath Routing for Mobile Ad Hoc Networks ," *IEEE ICCCN 1999*, pp. 64-70.

[15] C. E. Perkins and E. Royer, "Ad hoc on demand distance vector routing," *Proc. 2nd IEEE Workshop o Mobile Computing Systems and Applications*, Feb 1999.

[16] J. G. Proakis, *Digital Communications (4nd Edition)* Kluwer AcMcGraw-Hill Higher Education, New York, 2001.

[17] G. L. Stuber, *Principles of Mobile Communication (2nd Edition)* Kluwer Academic Press, 2001.

[18] A. Tsirigos, and Z.J. Haas, " Multipath routing in mobile ad hoc networks or how to route in the presence of frequent topology changes ," *IEEE MILCOM 2001*, pp. 878-883.

[19] L. Wang, Y.T. Shu, M. Dong, L.F. Zhang, and W.W. Yang, " Multipath Source Routing in wireless Ad Hoc Networks ," *Canadian Conference on Electrical and Computer Engineering*, vol. 1, pp. 479-483, 2000

[20] S. B. Wicker, *Error Control Systems for Digital Communication and Storage*, Prentice Hall, Upper Saddle River, NJ, 1995.

Fault-tolerant and Energy Efficient Cross-Layer Design for Wireless Sensor Networks

Qilian Liang and Lingming Wang

Department of Electrical Engineering

University of Texas at Arlington

Arlington, TX 76019-0016 USA

E-mail: liang@uta.edu, wang@wcn.uta.edu

Abstract

In wireless sensor networks, Fault-tolerant and energy efficiency are two important topics. Some link failure may happen during data transmission, and some threat can come from compromised nodes, which might relay incorrect information (packet) to the next node during routing. Traditional security mechanisms are not sufficient by themselves for this attack. Retransmission or detection of such incorrect information is very difficult. In this paper, we propose a Fault-tolerant and Energy Efficient Multipath-routing (FEEM) scheme aided with channel coding and interleaver. The multipath are chosen using a distributed geographical routing which is based on fuzzy logic system considering the remaining battery capacity, mobility, and distance to the destination node. Simulation results show that even if certain paths have failure or are compromised, the receiver node is still able to recover the transmitted message from failure with very low bit error rate.

Index Terms : Wireless sensor networks, multipath routing, energy efficiency, security, fault-tolerant, channel coding.

1 Introduction

Wireless sensor networking is an emerging technology that promises unprecedented ability to monitor and manipulate the physical world via a network of densely distributed wireless sensor nodes. The nodes can sense the physical environment in a variety of modalities, including acoustic, video, seismic, thermal, and infrared, etc. In wireless sensor networks, there exists some challenges:

- The routing path (link) failure may happen during data transmission because of collision, node dying out (no battery), node busy, or other accidents. Some applications require real time information and data, which means re-transmission is not possible.

- Security is an important topic for sensor networks, especially for the security-sensitive applications such as battlefield monitoring and homeland security. Traditional security mechanisms, such as authentication protocols, digital signature, and encription, can play important roles in achieving confidentiality, integrity, authentication, and non-repudiation of communication in ad hoc networks, but these mechanisms are not sufficient by themselves for mobile sensor networks.

- There exists energy constraint in wireless sensor networks because most sensors are battery operated, which means the operating signal-to-noise-ratio (SNR) is very low, and some energy efficiency schemes have to be developped.

These challenges motivate us to design a fault-tolerant (tolerate link failure and compromised nodes) and energy efficient schemes for information and data transmission in wireless

sensor networks. In this paper, we propose a Fault-tolerant and Energy Efficient Multipath-routing (FEEM) scheme aided with channel coding and interleaver in wireless sensor networks, which is a cross-layer approach.

Many routing protocols have been developed for ad hoc networks, which can be summarized as two categories: table-driven (e.g., destination sequenced distance vector [1], cluster switch gateway routing [3]) and source-initiated on-demand-driven (e.g., ad hoc on-demand distance vector routing [18], dynamic source routing [9]). In [12], Lee and Gerla proposed a Split Multipath Routing protocol that builds maximal disjoint paths, where data traffic is distributed in two roots per session to avoid congestion and to use network resources efficiently. A Multipath Source Routing (MSR) scheme was proposed in [24], which is an extension of Dynamic Source Routing (DSR). Their work focuses on distributing load adaptively among several paths. Nasipuri and Das [17] presented the On-Demand Multipath Routing scheme, which is also an extension of DSR. In their scheme, alternative routes are maintained, which can be utilized when the primary one fails. Tsirigos and Haas [22] proposed a multipath routing scheme based on Diversity Coding. Three different paths are utilized to distribute the data, and x-for-y Diversity Coding is used to offer protection against at most x lost blocks out of the total $x + y$ blocks. Security in ad hoc networks and sensor networks have been studied by some researchers. Zhou and Haas [27] took advantage of inherent redundancy in ad hoc networks – multiple routes between nodes – to defend routing against denial of service attacks. Law et al [11] benchmarked some well-known cryptographic algorithms in search for the best compromise in security and energy efficiency on a typical sensor node. Deng et al [4] evaluated the performance of INSENS, an INtrusion-tolerant routing protocol for wireless SEnsor Networks. Karlof and Wagner [10] considered routing security in wireless sensor networks. However, none of these security-related approaches considered to solve this problem from physical layer design. In additions, energy efficient routing has been exten-

sively studied by this community. In [26], a location-aided power aware routing protocol was proposed. Singh et al [20] proposed power-aware routing and discussed different metrics in power-aware routing; Li et al [13] extended their work and proposed an online power aware routing in wireless ad-hoc networks.

The rest of the paper is organized as follows. In Section 2, we present a distributed geographical multipath routing in a wireless sensor network. In Section 3, we present our fault-tolerant and energy efficient multipath-routing (FEEM) scheme Aided with Channel Coding and Interleaver. The simulation results and performance analysis are presented in Section 4, and in Section 5, we conclude this paper.

2 DIstributed Geographical Multipath-routing (DIGM)

In this paper, we propose a DIstributed Geographical Multipath-routing (DIGM) scheme to set M-path (for multipath routing). In the existing geographical routing approach (e.g., [7]), the path selection doesn't consider the remaining battery capacity of each node and its mobility, which are two very important factors for energy efficiency and network lifetime. Sensor mobility means the degree of channel fading, and high mobility requires higher signal-to-noise ratio for operating if the bit-error-rate (BER) or frame-error-rate (FER) requirements are given. In our DIGM, we consider *distance to the sensor node*, *remaining battery capacity*, and *mobility of each sensor*. The geographical location of destination sensor is known (as in [7]), and the physical location of each sensor node can be estimated easily if the locations of three sensor nodes (within a communication/sensing range) are known. Our scheme is a fully distributed approach where each sensor only needs the above three parameters, and we use fuzzy logic systems to handle these three parameters in the DIGM.

2.1 Overview of Fuzzy Logic Systems

Figure 1 shows the structure of a fuzzy logic system (FLS) [15]. When an input is applied to a FLS, the inference engine computes the output set corresponding to each rule. The defuzzifer then computes a crisp output from these rule output sets. Consider a p-input 1-output FLS, using singleton fuzzification, *center-of-sets* defuzzification [16] and "IF-THEN" rules of the form

$$R^l : \text{IF } x_1 \text{ is } \mathrm{F}_1^l \text{ and } x_2 \text{ is } \mathrm{F}_2^l \text{ and } \cdots \text{ and } x_p \text{ is } \mathrm{F}_p^l, \text{ THEN } y \text{ is } \mathrm{G}^l.$$

Assuming singleton fuzzification, when an input $\mathbf{x}' = \{x_1', \ldots, x_p'\}$ is applied, the degree of firing corresponding to the lth rule is computed as

$$\mu_{\mathrm{F}_1^l}(x_1') \star \mu_{\mathrm{F}_2^l}(x_2') \star \cdots \star \mu_{\mathrm{F}_p^l}(x_p') = \mathcal{T}_{i=1}^{p} \mu_{\mathrm{F}_i^l}(x_i') \tag{1}$$

where $\star$ and $\mathcal{T}$ both indicate the chosen t-norm. There are many kinds of defuzzifiers. In this paper, we focus, for illustrative purposes, on the center-of-sets defuzzifier [16]. It computes a crisp output for the FLS by first computing the centroid, c_{G^l}, of every consequent set G^l, and, then computing a weighted average of these centroids. The weight corresponding to the lth rule consequent centroid is the degree of firing associated with the lth rule, $\mathcal{T}_{i=1}^{p} \mu_{\mathrm{F}_i^l}(x_i')$, so that

$$y_{cos}(\mathbf{x}') = \frac{\sum_{l=1}^{M} c_{\mathrm{G}^l} \mathcal{T}_{i=1}^{p} \mu_{\mathrm{F}_i^l}(x_i')}{\sum_{l=1}^{M} \mathcal{T}_{i=1}^{p} \mu_{\mathrm{F}_i^l}(x_i')} \tag{2}$$

where M is the number of rules in the FLS.

2.2 FLS for Node Selection in Multipath Routing

In our DIGM, the source node select M nodes in its communication range for the first hop relay. Assume there are N $(N > M)$ nodes in its communication range, nodes who are further to the destination node than the source node are not considered. Picking M nodes

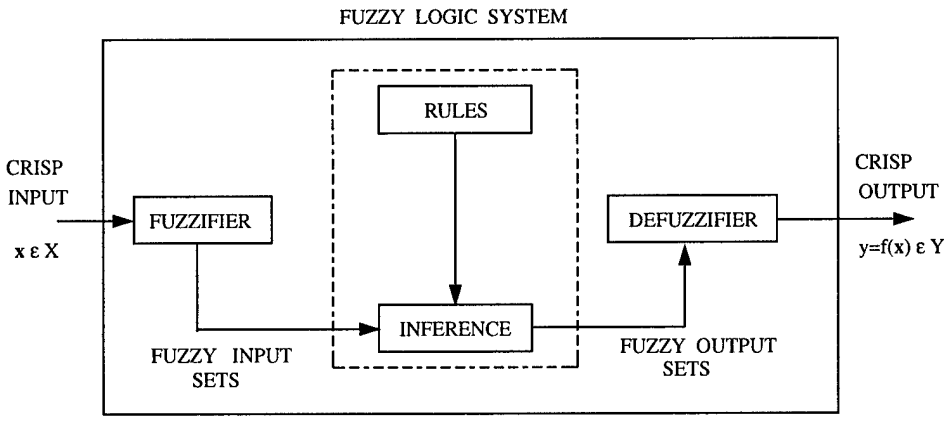


Figure 1: The structure of a fuzzy logic system.

from remaining eligible nodes is based on a FLS (as will be described in detail). In the second hop, each node in the M nodes will select its next hop node also using a FLS.

In our FLS design, we set up fuzzy rules for node selection based on the following three descriptors:

1. distance of a node to the destination,

2. its remaining battery capacity, and

3. its degree of mobility.

The linguistic variables used to represent the distance of a node to the destination were divided into three levels: *near*, *moderate*, and *far*; and those to represent its remaining battery capacity and degree of mobility were divided into three levels: *low*, *moderate*, and *high*. The consequent – the possibility that this node will be selected – was divided into 5 levels, *Very Strong, Strong, Medium, Weak, Very Weak*. So we need to set up $3^3 = 27$ (because every antecedent has 3 fuzzy sub-sets, and there are 3 antecedents) rules for this FLS.

A desired node to be included into the path should have near distance to the destination, high remaining battery capacity (so that the network life can last longer), and low mobility

(so that channel fading will not be severe). Based on this fact, we design a fuzzy logic system using rules summarized in Table 1.

We used trapezoidal membership functions (MFs) to represent *near*, *low*, *far*, and *high*, and triangle MFs to represent *moderate*. We show these MFs in Fig. 2a.

For every input (x_1, x_2, x_3), the output is computed using

$$y(x_1, x_2, x_3) = \frac{\sum_{l=1}^{27} \mu_{\mathrm{F}_l^1}(x_1)\mu_{\mathrm{F}_l^2}(x_2)\mu_{\mathrm{F}_l^3}(x_3)c^l}{\sum_{l=1}^{27} \mu_{\mathrm{F}_l^1}(x_1)\mu_{\mathrm{F}_l^2}(x_2)\mu_{\mathrm{F}_l^3}(x_3)} \tag{3}$$

where c^l is the centroid of consequent set. The output from FLS is degree of the possibility that this node will be selected into the path.

Initially, the source node uses a FLS to evaluate all eligible nodes (closer to the destination location) in its communication range based on the parameters of each node: distance to the destination, remaining battery capacity, and degree of mobility. The source node choose the top M nodes based on the degree of the possibility that this node will be selected into each path (totally M paths). In the second hop, the selected node in each path will choose its next hop node uses a FLS. As illustrated in Fig. 3, node B needs to choose one node from eligible nodes C, D, E, F, H based on their three parameters. If the top one node is unavailable (selected by another path or busy), then the top second node will be selected. By this means, M paths can be set up.

3 Fault-Tolerant and Energy Efficient Multipath-routing (FEEM) Aided with Channel Coding and Interleaver

In our fault-tolerance, we will tolerate link failure and security-related problems. In the security part, there are two sources of threats to routing protocols. The first comes from external attacks. By injecting erroneous routing information, replaying old routing informa-

tion, or distorting routing information, an attacker could successfully partition a network or introduce excess traffic load into the network by causing retransmission and inefficient routing. This kind of attack can be overcome using cryptographic schemes such as digital signature to protect the routing information [27]. The second and also the more severe kind of threats comes from compromised nodes, which might relay incorrect information (packet) to the next node during routing. Detection of such incorrect information is difficult: merely requiring relayed information to be signed by each node would not work because compromised nodes are able to generate valid signatures using their private keys. In this paper, we focus on the second threat and our goal is: even if certain paths are compromised, the receiver node may still be able to recover message from errors. In this paper, we propose a Fault-tolerant and Energy Efficient Multipath-routing (FEEM) scheme aided with channel coding and interleaver.

In our FEEM with channel coding and interleaver scheme. We apply convolutional coding to encode the information bits, then the code words are interleaved. Interleaver [25] was used to eliminate the correlation of the noise/fading process affecting adjacent symbols in a received code word, but here we use interleaver to make sure that the incorrect symbols in one compromised path will be spreaded after de-interleaver so that the Viterbi decoder will perform well. The interleaved bits are inserted with some unique words (for demodulation purpose), and then these bits are modulated to symbols. By this means, a frame has been built. For M-path routing, we split the symbols in one frame to M equal-length bursts, and each path transmits one burst in parallel. The receiver node demodulates each received burst from different path and provide soft-decision output. The receiver node combines all the soft-decision output from each burst according to the order when they are transmitted. In this paper, we use the demodulation algorithm we proposed in [14] for soft decision output. In case one or more bursts are lost due to link failure during transmission, the receiver

node will provide 0's as the soft decision output. Then de-interleaving is performed to the soft-decision output, and the de-interleaved data are used as the input to Viterbi decoder. The decoded output from Viterbi decoder are the information bits with possible errors due to compromised nodes (providing random data relay) and additive white Gaussian noise (AWGN). We summarize this scheme using a diagram in Fig. 4.

4 Simulations and Performance Analysis

4.1 Sensor Mobility and Channel Fading

Mobility of a sensor generates a doppler shift, which is a key parameter of fading channel. The doppler shift is

$$f_d = \frac{v}{c} f_c \tag{4}$$

where v is the speed of a sensor, c is the speed of light ($3 \times 10^8 m/s$), and f_c is the carrier. In our simulation, we used the carrier is $5GHz$. For reference, if a sensor moves with speed $12m/s$, the doppler shift is $200Hz$.

We model channel fading in sensor networks as Rician fading. Rician fading occurs when there is a strong specular (direct path or line of sight component) signal in addition to the scatter (multipath) components. For example, in communication between two infraed sensors, there exist a direct path. The channel gain,

$$g(t) = g_I(t) + j g_Q(t) \tag{5}$$

can be treated as a wide-sense stationary complex Gaussian random process, and $g_I(t)$ and $g_Q(t)$ are Gaussian random processes with non-zero means $m_I(t)$ and $m_Q(t)$, respectively; and they have same variance σ_g^2, then the magnitude of the received complex envelop has a

Rician distribution,

$$p_\alpha(x) = \frac{x}{\sigma^2}\exp\{-\frac{x^2+s^2}{2\sigma^2}\}I_0(\frac{xs}{\sigma^2}) \quad x \geq 0 \tag{6}$$

where

$$s^2 = m_I^2(t) + m_Q^2(t) \tag{7}$$

and $I_0(\cdot)$ is the zero order modified Bessel function. This kind of channel is known as Rician fading channel. A Rician channel is characterized by two parameters, Rician factor K which is the ratio of the direct path power to that of the multipath, i.e., $K = s^2/2\sigma^2$, and the Doppler spread (or single-sided fading bandwidth) f_d. We simulate the Rician fading using a direct path added by a Rayleigh fading generator. The Rayleigh fade generator is based on Jakes' model [8] in which an ensemble of sinusoidal waveforms are added together to simulate the coherent sum of scattered rays with Doppler spread f_d arriving from different directions to the receiver. The amplitude of the Rayleigh fade generator is controlled by the Rician factor K. The number of oscillators to simulate the Rayleigh fading is 60.

4.2 Performance of FEEM for Link Failure

We evaluated our FEEM scheme using computer simulations. We ran our simulations for four-path FEEM and six-path transportation FEEM, and assumed each path has 2% failure rate. QPSK modulation and convolutional codes with rate $\frac{1}{2}$ and connections 101 and 111 (in binary) were used in the transmitting sensor (encoder) and receiver node (Viterbi decoder).

For four-path FEEM, the frame structure is plotted in Fig. 6 (a) with 820 QPSK symbols (800 symbols payload and 20 symbols UW) were used. We used block interleaver with size 8×200 to interleave the payload bits (after channel coding), The interleaver and de-interleaver is shown in Fig. 5ab where $M = 4$ in this paper. Then we construct a frame by inserting UW and modulation. One frame is splitted to four equal-length bursts ($205 sym/burst$) for transmission. We ran Monte-Carlo Simulations for 10^5 frames at each E_b/N_0 value,

and compared its performance against 2-path diversity. In 2-path diversity, the transmitted symbols in each path are identical, but it will have big advantage if one path has failure during transportation. In the simulation, the frame in each path has 400 payload symbols and 10 UW symbol per burst without coding (illustrated in Fig. 6(b)). Considering two paths, the total number of symbols (820 symbols) is the same as the FEEM per transportation.

In Fig. 7, we summarized the average bit error rate (BER) versus E_b/N_0. Observe that the FEEM scheme has more than 3dB gain comparing to the 2-path diversity scheme. It clearly shows a BER floor for the FEEM scheme at high E_b/N_0 because there exists 2% failure rate for each path. But the performance of our FEEM is very good (e.g., $BER = 3 \times 10^{-4}$ at $E_b/N_0 = 5dB$).

In mobile wireless sensor networks, there exists channel fading during data transportation. In the simulation, we used Rician fading $K = 9dB$ and $f_d = 20Hz$. We compared our FEEM scheme against the two-path diversity with maximal ratio combination (MRC) scheme. Diversity is very powerful in combatting channel fading [21], and MRC is the optimal combination scheme for diversity. We used the same frame structure as that in dual transportation scheme (Fig. 6b). We ran Monte-Carlo Simulations for 2×10^5 frames at each E_b/N_0 value for four-path FEEM and diversity with MRC, and summarized the results in Fig. 8. Observe that four-path FEEM can achieve more than $1dB$ gain at $BER = 10^{-3}$.

In six-path FEEM, the frame structure is plotted in Fig. 9 (a) with 930 QPSK symbols (900 symbols payload and 30 symbols UW) were used. We used block interleaver with size 12×150 to interleave the payload bits (after channel coding), and then then construct a frame by inserting UW and modulation. One frame is splitted to six equal-length bursts ($155sym/burst$) for transmission.

We ran Monte-Carlo Simulations for 10^5 frames at each E_b/N_0 value, and compared its performance against the 2-path diversity. The frame structure is provided in Fig. 9(b). In

Fig. 7, we plotted the average BER versus E_b/N_0. Observe that more than 4 dB gain can be achieved using FEEM.

Similarly, we performed simulations for Rician fading channel $K = 9dB$ and $f_d = 20Hz$, and compared our six-path FEEM against the two-path diversity with MRC. The simulation results are summarized in 8, which demonstrates that more than 2 dB gain can be achieved using six-path FEEM. Observe Fig. 7, and Figs. 8, for larger number of paths in FEEM, the performance is better, which means the fault is more tolerable.

We also simulated the frame-error-rate (FER) versus SNR. In Figs. 10(a)(b), we plotted the BER and FER versus SNR for Rician fading channel $K = 15dB$, $f_d = 10Hz$, respectively. Observe Fig. 10b, 1.5dB gain can be achieved at $FER = 2\%$.

4.3 Performance of FEEM for Compromised Nodes

Due to space limitation, we only include the performance for secure multipath routing where each path has 1% probability to be compromised. When a path is compromised, the received burst from this path is some data with random value. We evaluated our FEEM scheme using computer simulations. We ran our simulations for six-path SEEM aided with channel coding and interleaver. We assumed that each path has probability 1% to be compromised. QPSK modulation and convolutional codes with rate $\frac{1}{2}$ and connections 101 and 111 (in binary) were used in the transmitting sensor (encoder) and receiver node (Viterbi decoder). We used the frame structure plotted in Fig. 9 (a) for six-path FEEM. Block interleaver 12×300 (in bits) is used before modulation, and de-interleaver 300×12 (in soft-decision symbol with resolution 3 bits per symbol) is used after demodulation.

In our channel coding, we introduced some redundancy (coding rate 1/2), so we compared our FEEM scheme against 2-path diversity, which means both schemes introduced the same amount of redundancy. The frame structure of each path in the 2-path diversity is plotted

in Fig. 9 (b).

We ran Monte-Carlo Simulations for 10^5 frames at each E_b/N_0 value for our FEEM scheme and diversity with MRC. We evaluated a four-path FEEM for Rician fading channel with random K from 9dB–12dB and random f_d from 10Hz–200Hz, and each path has 1% probability to be compromised. We ran Monte-Carlo Simulations for 10^5 frames at each E_b/N_0 value for our SEEM scheme and diversity with MRC, and the channel fading is different from frame to frame. In Fig. 11, we summarized the average bit error rate (BER) versus E_b/N_0. Observe that about $1.4dB$ gain can be achieved at $BER = 0.5\%$. We also evaluated a six-path FEEM for Rician fading channel with random K from 9dB–12dB and random f_d from 10Hz–200Hz, and the BER is plotted in Fig. 12. Observe that about 3dB gain cab be achieved at $BER = 0.5\%$.

4.4 Energy Efficiency-Related Network Lifetime

In our simulation, we used a 50-node wireless sensor network where nodes are randomly distributed between $(x = 0, y = 0)$ and $(x = 650m, y = 500m)$; each node has random battery level between J to $10J$ and an unlimited amount of data to communicate; and each node is mobile with different velocity from 0 to $12m/s$. Assume that a node will reverse its moving direction if it reaches the border.

We used the burst format in Fig. 6 for four-path FEEM and two-path diversity. We used the same model as in [6] for the radio hardware energy dissipation where the transmitter dissipates energy to run the radio electonics and the power amplifier, and the receiver dissipates energy to run the radio electronics. We chose the path-loss exponent $p = 2$. To transmit an l-symbol message a distance d, the radio expends:

$$E_{Tx}(l, d) = E_{Tx-elec}(l) + E_{Tx-amp}(l, d) = lE_{elec} + l\epsilon d^2 \tag{8}$$

and to receive this message, the radio expends

$$E_{Rx}(l) = E_{Rx-elec}(l) = lE_{elec} \tag{9}$$

The electronics energy, E_{elec}, as described in [6], depends on factors such as coding, modulation, pulse-shaping and matched filtering; and the amplifier energy, ϵd^2 depends on the distance to the receiver and the acceptable bit error rate. In this paper, we chose: $E_{elec} = 50nJ/sym$, $\epsilon = 10pJ/sym/m^2$. Same as [6][23], the energy for data aggregation is set as $E_{DA} = 5nJ/sym/signal$.

We applied our FEEM to this senario. Energy is consumed whenever a node transmits or receives data or performs data aggregation. When a node uses up its energy, it dies out. Since the initial node locations and battery capacities were random, we ran Monte-Carlo simulations for 1000 times. We compared our FEEM algorithm against the two-path diversity where the two paths were selected just based on the minimum distance, as plotted in Fig. 13. From this figure, we see that our scheme performs much better than the minimum distance scheme.

4.5 Performance Analysis

Why our FEEM scheme can perform very well even with 2% link failure or 1% to be compromised in each path? This can be explained based on the successful example of puncturing. Puncturing is often used to generate additional rates from a single convolutional code [2][5]. The basic idea behind puncturing is not to transmit some of the bits output by the convolutional encoder, thus increase the rate of the code. This increase in rate decrease the free distance of the code, but usually the resulting free distance is very close to the optimum one. The receiver inserts dummy bits to replace the punctured bits in the receiver, hence only one encoder/decoder pair is needed to generate several different code rates. In our

M-path routing, the receiver node inserts 0's if one burst is lost during transmission, or a compromised path provides random values to the receiver node. Then the receiver node de-interleaves the soft-decision output from demodulator (random value), which is very similar that some dummy bits are used to replace the bits from compromised path. But in our scheme, the effective puncturing pattern in terms of the number of bits and puncture location is time-varying from frame to frame.

5 Conclusions

In wireless sensor networks, the energy is limited, and some link failure may happen during data transmission. In additions, threat can come from compromised nodes, which might relay incorrect information (packet) to the next node during routing. Detection of such incorrect information is very difficult. In this paper, we proposed a FEEM aided with channel coding and interleaver scheme for wireless sensor networks to tolerate this. The M-path in multipath routing are selected using fuzzy logic systems considering the remaining battery capacity, mobility, and distance to the destination node. Based on the simulation reseults, we draw the following conclusions:

1. Our scheme performs much better than the diversity with MRC scheme in terms of BER.

2. Our FEEM can tolerate some link failures and compromised, which makes wireless sensor networks survivable and resilient.

3. Our FEEM scheme can work at low SNR (e.g., $E_b/N_0 = 5dB$), which can save lots of energy because energy constraint is one of the most important topics in wireless sensor networks, and existing studies show that most energy is consumed in communication-related activies in wireless sensor networks.

4. The larger the number of paths in FEEM, the better the performance, which means the fault is more tolerable.

5. The network lifetime can be extended using our FEEM scheme.

Acknowledgement

This work was supported by the U.S. Office of Naval Research (ONR) Young Investigator Program Award under Grant N00014-03-1-0466.

References

[1] C. P. Bhagwat, "Highly dynamic destination-sequenced distance vector routing," *Proc. of ACM SIGCOMM'94*, pp.234-244, Sept 1994.

[2] J. B. Cain, G. C. Clark Jr, and J. M. Geist, "Punctured convolutional codes of rate (n-1)/n and simplified maximum likelihood decoding," *IEEE Trans on Information Theory*, vol. 25, pp. 97-100, Jan 1979.

[3] C. -C. Chiang, et al, "Routing in clustered multihop mobile wireless networks with fading channel," *Proc. IEEE Singapore Intl Conference on Networks*, 1997.

[4] J. Deng, R. Han, S. Mishra, "A Performance Evaluation of Intrusion-Tolerant Routing in Wireless Sensor Networks," *IPSN 2003.*

[5] J. Hagenauer, "Rate compatible punctured convolutional codes and their applications," *IEEE Trans on Communications*, vol. 36, pp. 389-400, April 1988.

[6] W. B. Heinzelman, et al, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Trans on Wireless Communications*, vol. 1, no. 4, pp. 660-670, Oct 2002.

[7] R. Jain, A. Puri, and R. Sengupta, "Geographical routing using partial information for wireless sensor networks," *IEEE Personal Communications*, pp. 48-57, Feb 2001.

[8] W. C. Jakes, *Microwave Mobile Communication*, New York, NY: IEEE Press, 1993.

[9] D. Johnson and D. Maltz, *Mobile Computing*, Kluwer Academic Publishers, 1996.

[10] C. Karlof and D. Wagner, "Secure Routing in Sensor Networks: Attacks and Countermeasures," *SNPA 2003.*

[11] Y.W. Law, S. Dulman, S. Etalle and P. Havinga, "Assessing Security-Critical Energy-Efficient Sensor Networks," Department of Computer Science, University of Twente, Technical Report TR-CTIT-02-18, Jul 2002.

[12] S.J. Lee, and M. Gerla, " Split Multipath Routing with Maximally Disjoint Paths in Ad Hoc Networks ," *ICC 2001.*,

[13] Q. Li, J. Aslam, and D. Rus, "Online power-aware routing in wireless ad-hoc networks," *Proc. of Annual ACM/IEEE International Conf. on Mobile Computing and Networking (MobiCom)*, Rome, Italy, pp. 97-107, 2001.

[14] Q. Liang, "Optimal demodulator for satellite-based wireless ATM networks," *IEEE International Conference on Communications (ICC),* May 2003, Alaska.

[15] J. M. Mendel, "Fuzzy Logic Systems for Engineering : A Tutorial," *Proceedings of the IEEE*, vol. 83, no. 3, pp. 345-377, March 1995.

[16] J. M. Mendel, *Uncertain Rule-Based Fuzzy Logic Systems*, Prentice-Hall, Upper Saddle River, NJ, 2001.

[17] A. Nasipuri, and S.R. Das, " On-Demand Multipath Routing for Mobile Ad Hoc Networks ," *IEEE ICCCN 1999*, pp. 64-70.

[18] C. E. Perkins and E. Royer, "Ad hoc on demand distance vector routing," *Proc. 2nd IEEE Workshop o Mobile Computing Systems and Applications*, Feb 1999.

[19] J. G. Proakis, *Digital Communications (4nd Edition)* Kluwer AcMcGraw-Hill Higher Education, New York, 2001.

[20] S. Singh, M. Woo, and C. S. Raghavendra, "Power-aware routing in mobile ad hoc networks," *Proc. of Annual ACM/IEEE International Conf. on Mobile Computing and Networking (MobiCom)*, Dallas, TX, pp. 181-190, 1998.

[21] G. L. Stuber, *Principles of Mobile Communication (2nd Edition)* Kluwer Academic Press, 2001.

[22] A. Tsirigos, and Z.J. Haas, " Multipath routing in mobile ad hoc networks or how to route in the presence of frequent topology changes ," *IEEE MILCOM 2001*, pp. 878-883.

[23] A. Wang, et al, "Energy-scalable protocols for battery-operated microsensor networks," *Proc of IEEE Workshop on SIgnal Processing Systems (SiPS'99)*, Taipei, Taiwan, Oct 1999, pp. 483-492.

[24] L. Wang, Y.T. Shu, M. Dong, L.F. Zhang, and W.W. Yang, " Multipath Source Routing in wireless Ad Hoc Networks ," *Canadian Conference on Electrical and Computer Engineering*, vol. 1, pp. 479-483, 2000

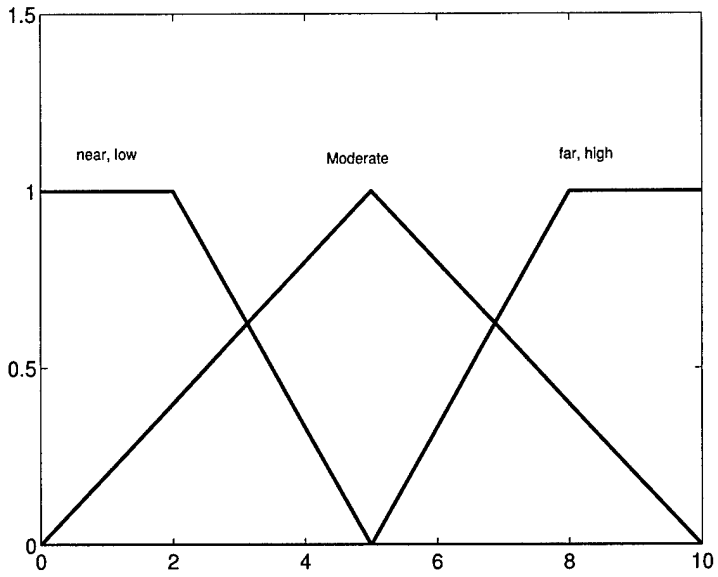
[25] S. B. Wicker, *Error Control Systems for Digital Communication and Storage*, Prentice Hall, Upper Saddle River, NJ, 1995.

[26] Y. Xue and B. Li, "A location-aided power-aware routing protocol in mobile ad hoc networks," *Proc. of Globecom'2001*, pp. 2837-2841, San Antonio, TX, Sept 2001.

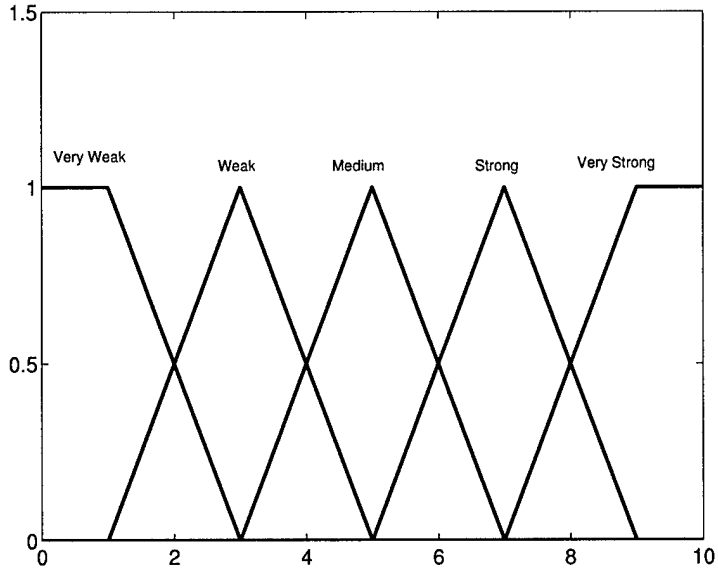
[27] L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks", *IEEE Networks, Special Issue on Network Security*, Nov/Dec 1999.

Table 1: The rules for node selection in multipath routing. Antecedent 1 is *distance of a node to the destination*, Antecedent 2 is *its remaining battery capacity*, Antecedent 3 is *its degree of mobility*, and Consequent is *the possibility that this node will be included into the path.*

Question #	Antecedent 1	Antecedent 2	Antecedent 3	Consequent
1	near	low	low	medium
2	near	low	moderate	weak
3	near	low	high	very weak
4	near	moderate	low	medium
5	near	moderate	moderate	strong
6	near	moderate	high	weak
7	near	high	low	very strong
8	near	high	moderate	strong
9	near	high	high	medium
10	moderate	low	low	weak
11	moderate	low	moderate	very weak
12	moderate	low	high	very weak
13	moderate	moderate	low	medium
14	moderate	moderate	moderate	medium
15	moderate	moderate	high	weak
16	moderate	high	low	strong
17	moderate	high	moderate	strong
18	moderate	high	high	weak
19	far	low	low	weak
20	far	low	moderate	very weak
21	far	low	high	very weak
22	far	moderate	low	weak
23	far	moderate	moderate	weak
24	far	moderate	high	very weak
25	far	high	low	medium
26	far	high	moderate	strong
27	far	high	high	medium



(a)



(b)

Figure 2: The MFs used to represent the linguistic labels. (a) MFs for antecedents, and (b) MFs for consequent.

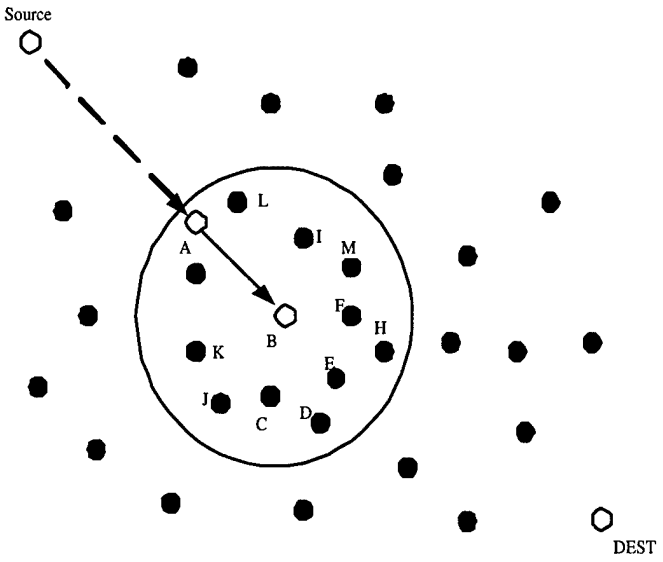


Figure 3: Illustration of node selection.

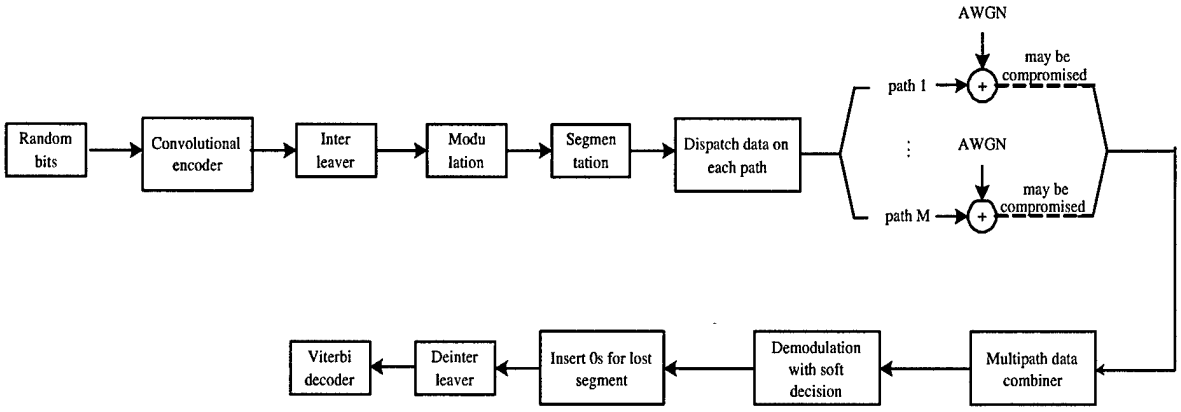
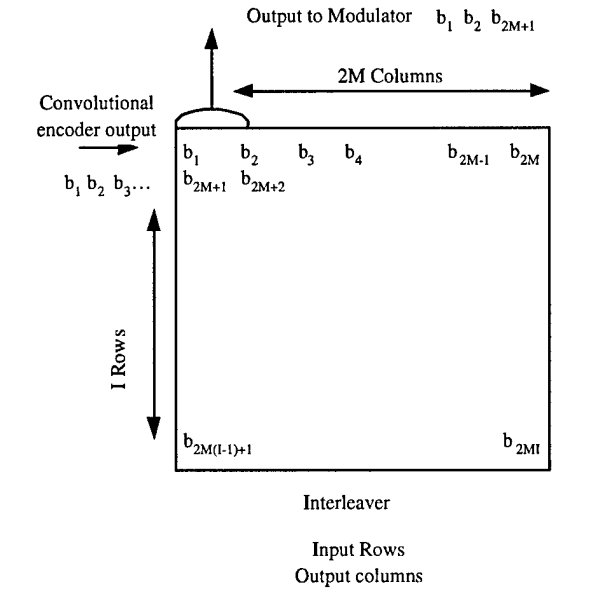
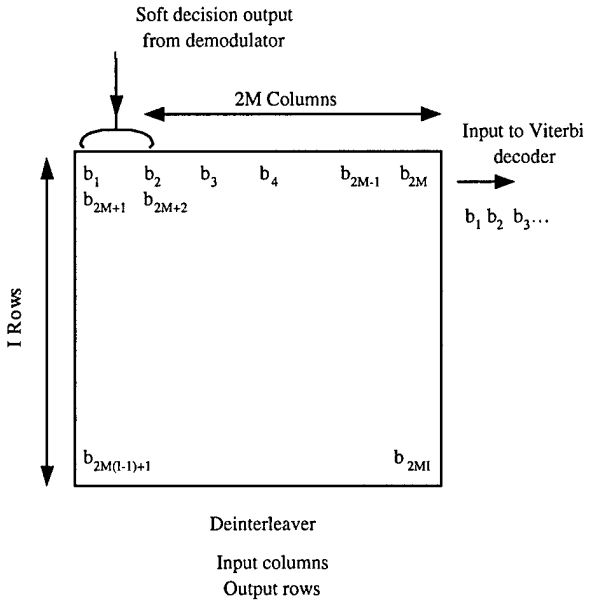


Figure 4: The diagram of FEEM aided with channel coding and interleaver.

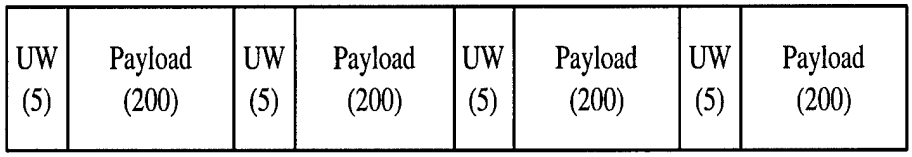


(a)

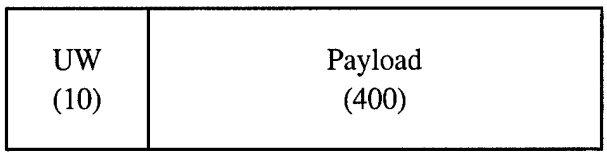


(b)

Figure 5: The interleaver and de-interleaver structures. (a) interleaver, and (b) de-interleaver.



(a)



(b)

Figure 6: Frame structure (in symbols) we used in our simulations. (a) Four-path FEEM, (b) 2-path diversity.

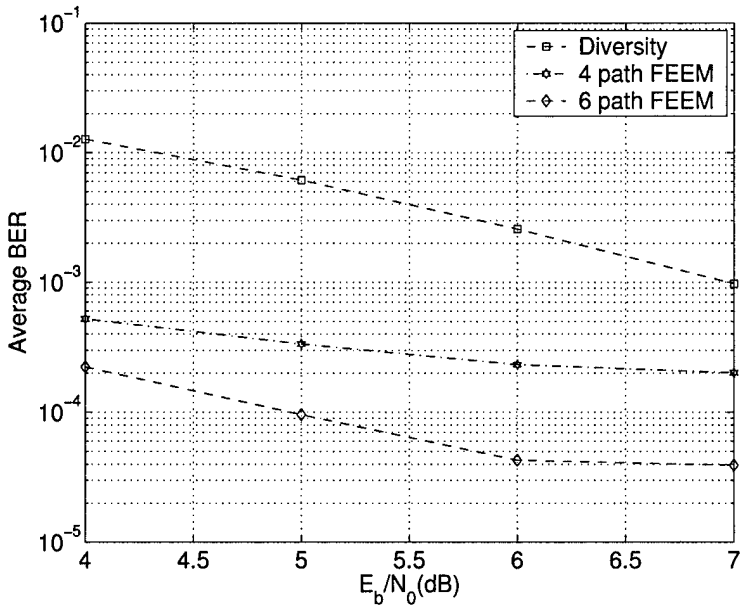


Figure 7: Average BER versus E_b/N_0 for four-path and six-path FEEM and 2-path diversity in static AWGN channel.

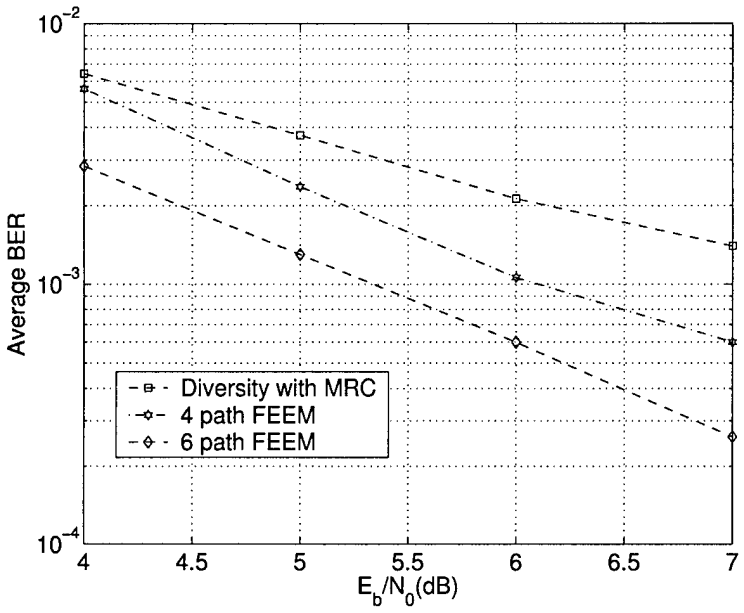
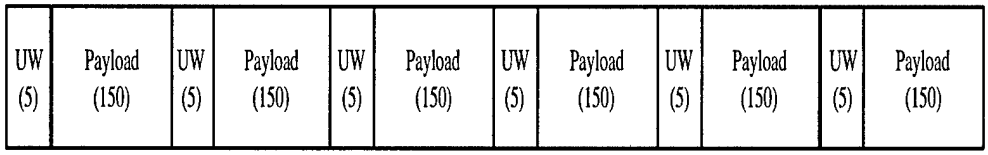
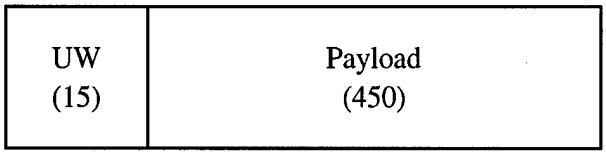


Figure 8: Average BER versus E_b/N_0 for FEEM and diversity with MRC in Rician fading channel ($K = 9dB, f_d = 20Hz$).

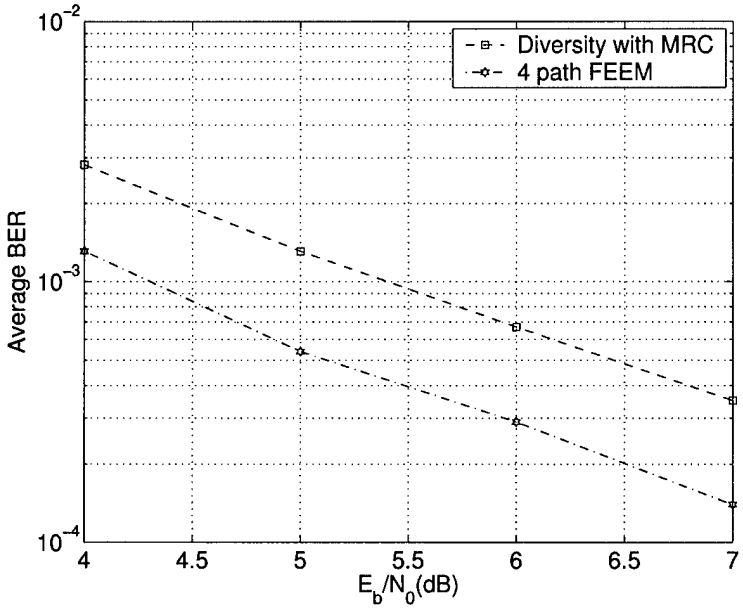


(a)

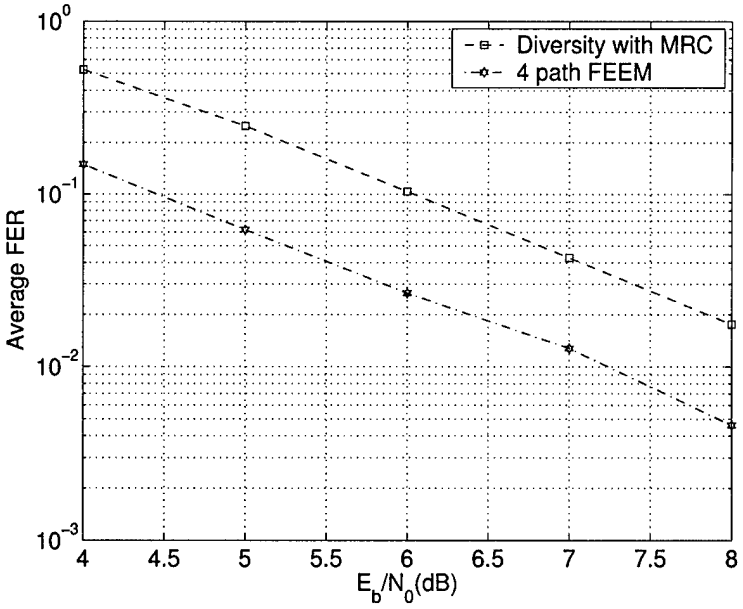


(b)

Figure 9: Frame structure (in symbols) we used in our simulations. (a) Six-path FEEM, (b) 2-path diversity.



(a)



(b)

Figure 10: Average BER and FER versus E_b/N_0 for FEEM and diversity with MRC in Rician fading channel ($K = 15dB, f_d = 10Hz$), (a) BER, and (b) FER.

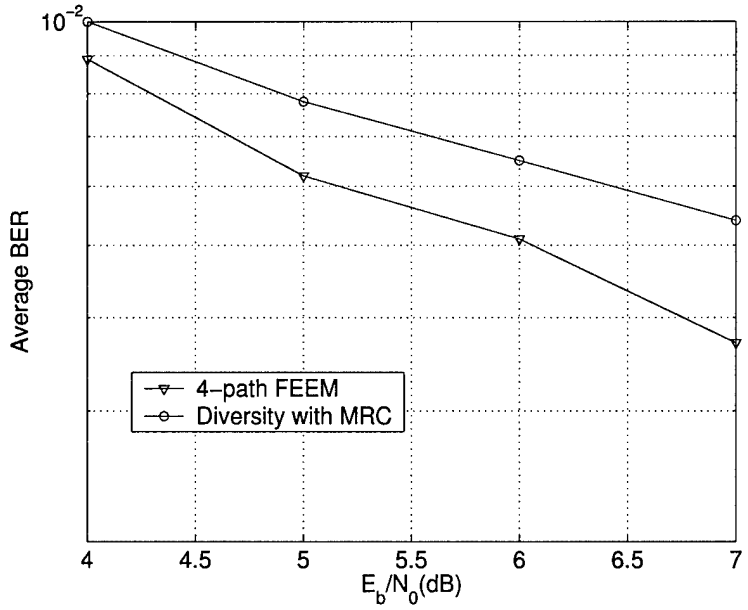


Figure 11: Average BER versus E_b/N_0 for four-path FEEM and diversity with MRC in Rician fading channel with random K from 9dB–12dB and random f_d from 10Hz–200Hz.

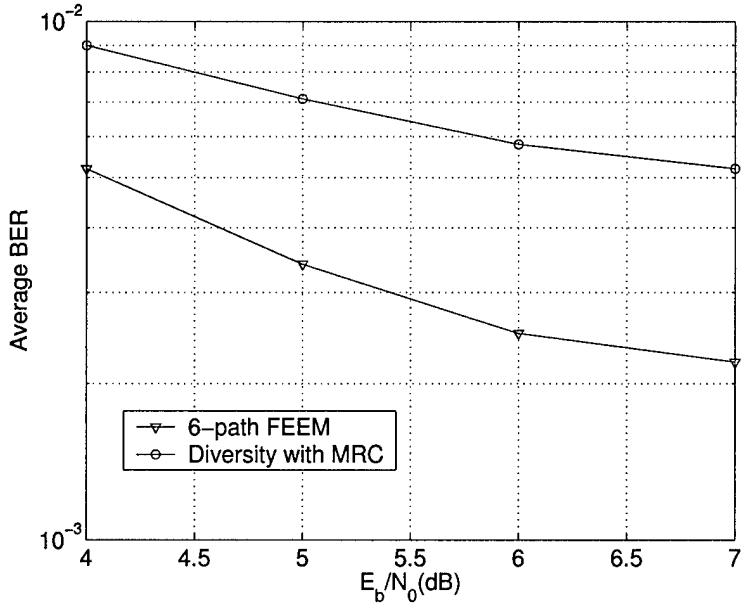


Figure 12: Average BER versus E_b/N_0 for six-path FEEM and diversity with MRC in Rician fading channel with random K from 9dB–12dB and random f_d from 10Hz–200Hz.

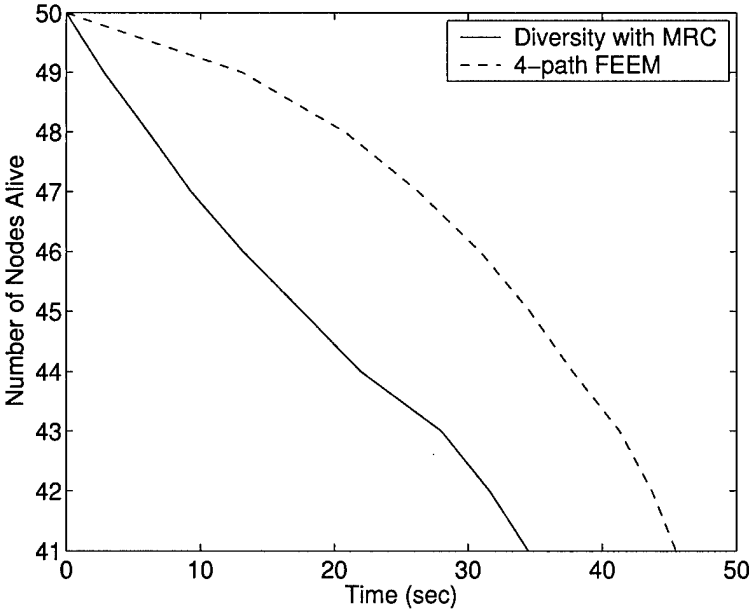


Figure 13: Time versus the number of nodes alive.

Secure and Energy Efficient Multipath-routing (SEEM) in Wireless Sensor Networks: A Cross Layer Approach

Qilian Liang and Lingming Wang
Department of Electrical Engineering
University of Texas at Arlington
Arlington, TX 76019-0016 USA
E-mail: liang@uta.edu, wang@wcn.uta.edu

Abstract— **In wireless sensor networks, security and energy efficiency are two important topics. In multipath routing, threat can come from compromised nodes, which might relay incorrect information (packet) to the next node during routing. Detection of such incorrect information is very difficult. In this paper, we propose a Secure and Energy Efficient Multipath-routing (SEEM) scheme aided with channel coding and interleaver. The M-path in multipath routing are selected using existing routing algorithm and fuzzy logic system considering the average remaining battery capacity and mobility of associated nodes. Simulation results show that even if certain paths are compromised, the receiver node is still able to recover the transmitted message from errors with very low bit error rate.**

Index Terms : Wireless sensor networks, security, multipath routing, energy efficiency, channel coding.

I. Introduction

Wireless sensor networking is an emerging technology that promises unprecedented ability to monitor and manipulate the physical world via a network of densely distributed wireless sensor nodes. The nodes can sense the physical environment in a variety of modalities, including acoustic, seismic, thermal, and infrared. Security is an important topic for sensor networks, especially for the security-sensitive applications such as battlefield monitoring and homeland security. Traditional security mechanisms, such as authentication protocols, digital signature, and encription, can play important roles in achieving confidentiality, integrity, authentication, and non-repudiation of communication in ad hoc networks, but these mechanisms are not sufficient by themselves for mobile sensor networks. Besides, energy efficiency is also very important for wireless sensor networks because most wireless sensor networks are battery-operated and it is impossible to be recharged once deployed.

Security in ad hoc networks and sensor networks have been studied by some researchers. Zhou and Haas [23] took advantage of inherent redundancy in ad hoc networks – multiple routes between nodes – to defend routing against denial of service attacks. Law et al [9] benchmarked some well-known cryptographic algorithms in search for the best compromise in security and energy efficiency on a typical sensor node. Deng et al [4] evaluated the performance of INSENS, an INtrusion-tolerant routing protocol for wireless SEnsor Networks. Karlof and Wagner [8] considered routing security in wireless sensor networks. However, none of these security-related approaches considered to solve this problem from physical layer design. Energy efficient routing has been extensively studied by this community. In [22], a location-aided power aware routing protocol was proposed. Singh et al [17] proposed power-aware routing and discussed different metrics in power-aware routing; Li et al [11] extended their work and proposed an online power aware routing in wireless ad-hoc networks. In this paper, we propose a Secure and Energy Efficient Multipath-routing (SEEM) scheme with the aid of channel coding and interleaver, which is a cross layer approach.

The rest of the paper is organized as follows. In Section II, we provide some preliminary knowledge. In Section III, we present our secure and energy efficient multipath-routing (SEEM) scheme Aided with Channel Coding and Interleaver. The simulation results and performance analysis are presented in Section IV, and in Section V, we conclude this paper.

II. Preliminaries

A. Candidate Paths in Multipath Routing

In our scheme, the candidate paths to be used for multipath (M-path) routing can be be chosen using existing routing algorithms. Many routing protocols have been developed for ad hoc sensor networks, which can be summarized as two categories: table-driven (e.g., destination sequenced distance vector [1], cluster switch gateway

routing [3]) and source-initiated on-demand-driven (e.g., ad hoc on-demand distance vector (AODV) routing [15], dynamic source routing (DSR) [7]). In [10], Lee and Gerla proposed a Split Multipath Routing protocol that builds maximal disjoint paths, where data traffic is distributed in two roots per session to avoid congestion and to use network resources efficiently. A Multipath Source Routing scheme was proposed in [20], which is an extension of Dynamic Source Routing. Their work focuses on distributing load adaptively among several paths. Nasipuri and Das [14] presented the On-Demand Multipath Routing scheme, which is also an extension of DSR. In their scheme, alternative routes are maintained, which can be utilized when the primary one fails. Tsirigos and Haas [19] proposed a multipath routing scheme based on Diversity Coding. Three different paths are utilized to distribute the data, and x-for-y Diversity Coding is used to offer protection against at most x lost blocks out of the total $x + y$ blocks. In this paper, we choose the M-path (for multipath routing) from N ($N > M$) candidate paths and the N candidate paths are obtained using AODV. In AODV, the path selection doesn't consider the remaining battery capacity of each node and its mobility. In selecting M paths from N candidates, we apply a fuzzy logic system (FLS) to paths selection considering the factors: the average remaining battery capacity and mobility of associated nodes.

B. Overview of Fuzzy Logic Systems

Figure 1 shows the structure of a fuzzy logic system (FLS) [13]. When an input is applied to a FLS, the inference engine computes the output set corresponding to each rule. The defuzzifer then computes a crisp output from these rule output sets. Consider a p-input 1-output FLS, using singleton fuzzification, *center-of-sets* defuzzification [13] and "IF-THEN" rules of the form

$$R^l : \text{IF } x_1 \text{ is } \mathrm{F}_1^l \text{ and } x_2 \text{ is } \mathrm{F}_2^l \text{ and } \cdots \text{ and } x_p \text{ is } \mathrm{F}_p^l, \text{ THEN } y \text{ is } \mathrm{G}^l.$$

Assuming singleton fuzzification, when an input $\mathbf{x}' = \{x_1', \ldots, x_p'\}$ is applied, the degree of firing corresponding to the lth rule is computed as

$$\mu_{\mathrm{F}_1^l}(x_1') \star \mu_{\mathrm{F}_2^l}(x_2') \star \cdots \star \mu_{\mathrm{F}_p^l}(x_p') = \mathcal{T}_{i=1}^{p} \mu_{\mathrm{F}_i^l}(x_i') \quad (1)$$

where $\star$ and $\mathcal{T}$ both indicate the chosen t-norm. There are many kinds of defuzzifiers. In this paper, we focus, for illustrative purposes, on the center-of-sets defuzzifier [13]. It computes a crisp output for the FLS by first computing the centroid, c_{G^l}, of every consequent set G^l, and, then computing a weighted average of these centroids. The weight corresponding to the lth rule consequent centroid is the degree of firing associated with the lth rule, $\mathcal{T}_{i=1}^{p} \mu_{\mathrm{F}_i^l}(x_i')$, so that

$$y_{cos}(\mathbf{x}') = \frac{\sum_{l=1}^{M} c_{\mathrm{G}^l} \mathcal{T}_{i=1}^{p} \mu_{\mathrm{F}_i^l}(x_i')}{\sum_{l=1}^{M} \mathcal{T}_{i=1}^{p} \mu_{\mathrm{F}_i^l}(x_i')} \quad (2)$$

where M is the number of rules in the FLS. In this paper, we apply a FLS for routes selection in multipath routing.

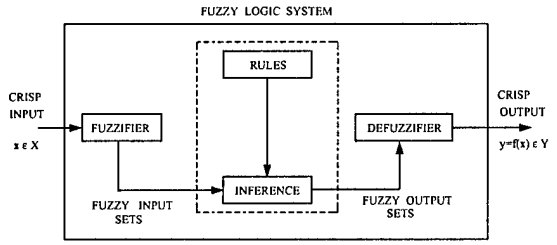


Fig. 1. The structure of a fuzzy logic system.

III. Secure and Energy Efficient Multipath-routing (SEEM) Aided with Channel Coding and Interleaver

A. M-Path Selection

In this paper, we choose the M-path (for multipath routing) from N ($N > M$) candidate paths and the N candidate paths are obtained using AODV. In AODV, the path selection doesn't consider the remaining battery capacity of each node and its mobility. In selecting M paths from N candidates, we apply a fuzzy logic system (FLS) to paths selection considering the factors: number of hops, remaining battery capacity of associated nodes, and mobility of associated nodes.

In AODV, the path selection already considered the number of hops, and the N selected paths are chosen based on this criterion. We further select M paths from the N paths ($M < N$) considering the remaining battery capacity and mobility of associated nodes using fuzzy logic system. The path is selected based on two descriptors: *the average remaining battery capacity of associated nodes*, and *the average mobility of associated nodes*. The linguistic variables used to represent the battery level and mobility were divided into three levels: *low*, *moderate*, and *high*. The consequent – the possibility that this path will be selected – was divided into 5 levels, *Very Strong, Strong, Medium, Weak, Very Weak*. We used trapezoidal membership functions (MFs) to represent *low*, *high*, *very strong*, and *very weak*; and triangle MFs to represent *moderate*, *strong*, *medium*, and *weak*. We show these MFs in Fig. 2ab.

A desired path should have high average remaining battery capacity so that the network life can last longer; and the average mobility of associated nodes should be low so that channel fading will not be very severe. Based

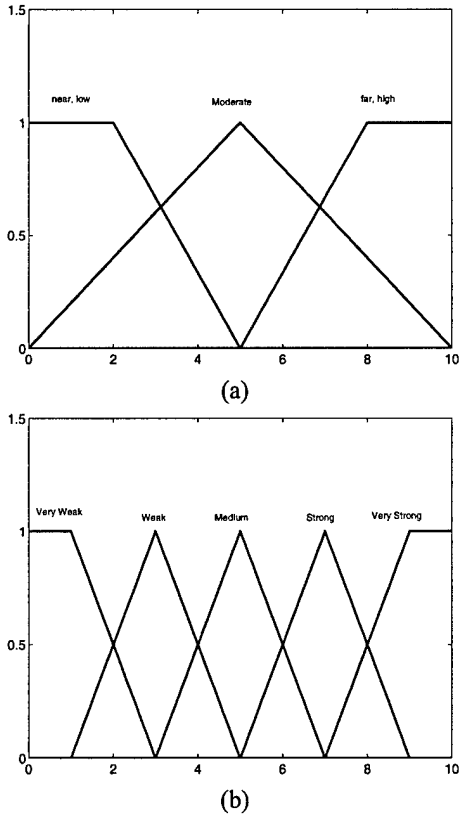


Fig. 2. The MFs used to represent the linguistic labels. (a) MFs for antecedents, and (b) MFs for consequent.

on this fact, we design a fuzzy logic system using rules such as:

R^l : IF *the average remaining battery capacity of associated nodes* (x_1) is F_l^1, and *the average mobility of associated nodes* (x_2) is F_l^2, THEN the possibility that this path will be selected (y) is G^l.

where $l = 1, \ldots, 9$. We summarize all the rules in Table I. For every input (x_1, x_2), the output is computed using

$$y(x_1, x_2) = \frac{\sum_{l=1}^{9} \mu_{\mathrm{F}_l^1}(x_1)\mu_{\mathrm{F}_l^2}(x_2)c_{avg}^l}{\sum_{l=1}^{9} \mu_{\mathrm{F}_l^1}(x_1)\mu_{\mathrm{F}_l^2}(x_2)} \quad (3)$$

For each path in the N candidate paths, a possibility (that this path will be selected) will be provided by the FLS, then the M paths with top possibilities are chosen for M-path routing.

B. Secure and Energy Efficient Multipath-routing Aided (SEEM) with Channel Coding and Interleaver

There are two sources of threats to routing protocols. The first comes from external attacks. By injecting erroneous routing information, replaying old routing information, or distorting routing information, an attacker could successfully partition a network or introduce excess traffic load into the network by causing retransmission and inefficient routing. This kind of attack can be overcome using cryptographic schemes such as digital signature to protect the routing information [23]. The second and also the more severe kind of threats comes from compromised nodes, which might relay incorrect information (packet) to the next node during routing. Detection of such incorrect information is difficult: merely requiring relayed information to be signed by each node would not work because compromised nodes are able to generate valid signatures using their private keys. In this paper, we focus on the second threat and our goal is: even if certain paths are compromised, the receiver node may still be able to recover message from errors.

TABLE I

THE RULES FOR M PATHS SELECTION. ANTECEDENT 1 IS *the average remaining battery capacity of associated nodes*, ANTECEDENT 2 IS *the average mobility of associated nodes*, AND CONSEQUENT IS *the possibility that this path will be selected.*

Rule #	Antecedent 1	Antecedent 2	Consequent
1	low	low	medium
2	low	moderate	low
3	low	high	very low
4	moderate	low	strong
5	moderate	moderate	medium
6	moderate	high	low
7	high	low	very strong
8	high	moderate	strong
9	high	high	medium

In our SEEM with channel coding and interleaver scheme. We apply convolutional coding to encode the information bits, then the code words are interleaved. Interleaver [21] was used to eliminate the correlation of the noise/fading process affecting adjacent symbols in a received code word, but here we use interleaver to make sure that the incorrect symbols in one compromised path will be spreaded after de-interleaver so that the Viterbi decoder will perform well. The interleaved bits are inserted with some unique words (for demodulation purpose), and then these bits are modulated to symbols. By this means, a frame has been built. For M-path routing, we split the symbols in one frame to M equal-length bursts, and each path transmits one burst in parallel. The receiver node demodulates each received burst from different path and provide soft-decision output. The receiver node combines all the soft-decision output from each burst according to the order when they are transmitted. In this paper, we use the demodulation algorithm we proposed in [12] for soft decision output. Then de-interleaving is performed to the soft-decision output, and the de-interleaved data are

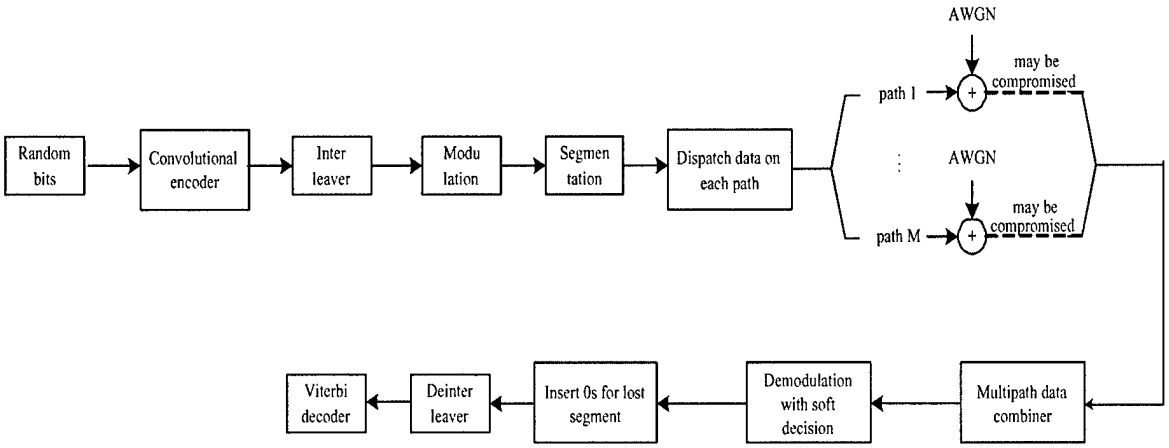


Fig. 3. The diagram of SEEM aided with channel coding and interleaver.

used as the input to Viterbi decoder. The decoded output from Viterbi decoder are the information bits with possible errors due to compromised nodes (providing random data relay) and additive white Gaussian noise (AWGN). We summarize this scheme using a diagram in Fig. 3.

IV. Simulations and Performance Analysis

A. Sensor Mobility and Channel Fading

Mobility of a sensor generates a doppler shift, which is a key parameter of fading channel. The doppler shift is

$$f_d = \frac{v}{c} f_c \tag{4}$$

where v is the speed of a sensor, c is the speed of light ($3 \times 10^8 m/s$), and f_c is the carrier. In our simulation, we used the carrier is $5GHz$. For your reference, if a sensor moves with speed $12m/s$, the doppler shift is $200Hz$.

We model channel fading in sensor networks as Rician fading. Rician fading occurs when there is a strong specular (direct path or line of sight component) signal in addition to the scatter (multipath) components. For example, in communication between two infraed sensors, there exist a direct path. The channel gain,

$$g(t) = g_I(t) + jg_Q(t) \tag{5}$$

can be treated as a wide-sense stationary complex Gaussian random process, and $g_I(t)$ and $g_Q(t)$ are Gaussian random processes with non-zero means $m_I(t)$ and $m_Q(t)$, respectively; and they have same variance σ_g^2, then the magnitude of the received complex envelop has a Rician distribution,

$$p_\alpha(x) = \frac{x}{\sigma^2} \exp\{-\frac{x^2+s^2}{2\sigma^2}\} I_0(\frac{xs}{\sigma^2}) \quad x \geq 0 \tag{6}$$

where

$$s^2 = m_I^2(t) + m_Q^2(t) \tag{7}$$

and $I_0(\cdot)$ is the zero order modified Bessel function. This kind of channel is known as Rician fading channel. A Rician channel is characterized by two parameters, Rician factor K which is the ratio of the direct path power to that of the multipath, i.e., $K = s^2/2\sigma^2$, and the Doppler spread (or single-sided fading bandwidth) f_d. We simulate the Rician fading using a direct path added by a Rayleigh fading generator. The Rayleigh fade generator is based on Jakes' model [6] in which an ensemble of sinusoidal waveforms are added together to simulate the coherent sum of scattered rays with Doppler spread f_d arriving from different directions to the receiver. The amplitude of the Rayleigh fade generator is controlled by the Rician factor K. The number of oscillators to simulate the Rayleigh fading is 60.

B. Performance of SEEM

Due to space limitation, we only include the performance for secure multipath routing where each path has 1% probability to be compromised. When a path is compromised, the received burst from this path is some data with random value. We evaluated our SEEM scheme using computer simulations. We ran our simulations for six-path SEEM aided with channel coding and interleaver. We assumed that each path has probability 1% to be compromised. QPSK modulation and convolutional codes with rate $\frac{1}{2}$ and connections 101 and 111 (in binary) were used in the transmitting sensor (encoder) and receiver node (Viterbi decoder). We used the frame structure plotted in Fig. 5 (a) for six-path SEEM. Block interleaver 12×300 (in bits) is used before modulation, and de-interleaver 300×12 (in soft-decision symbol with resolution 3 bits per symbol) is used after demodulation. The interleaver and de-interleaver structures are shown in Figs. 4ab where

$M = 6$ in this paper.

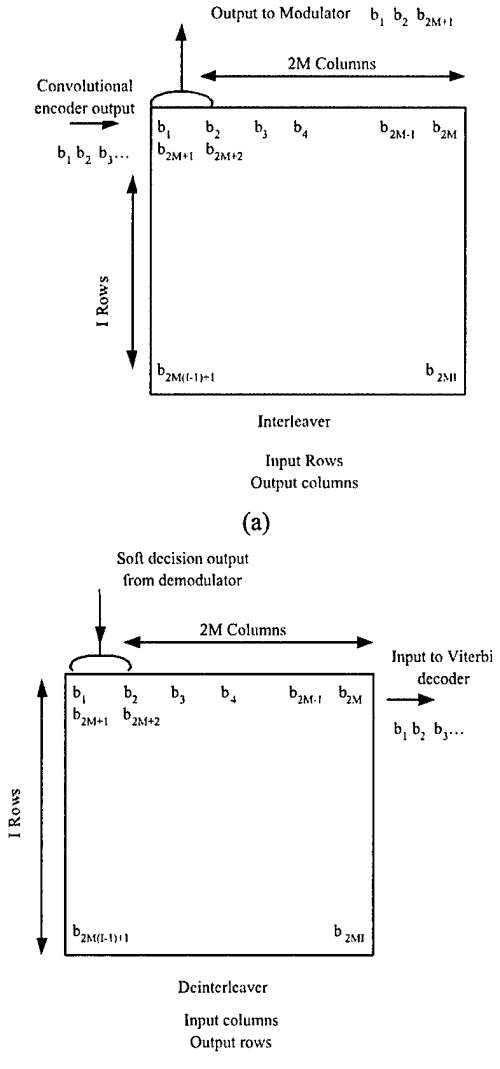


Fig. 4. The interleaver and de-interleaver structures. (a) interleaver, and (b) de-interleaver.

In our channel coding, we introduced some redundancy (coding rate 1/2), so we compared our SEEM scheme against 2-path diversity, which means both schemes introduced the same amount of redundancy. In this paper, we used maximal-ratio-combination (MRC) for diversity combining. MRC is known as the optimal combining scheme [18]. The frame structure of each path in the 2-path diversity is plotted in Fig. 5 (b).

We ran Monte-Carlo Simulations for 10^5 frames at each E_b/N_0 value for our SEEM scheme and diversity with MRC. In Fig. 6a, we summarized the average bit error rate (BER) versus E_b/N_0 for Rician fading channel $K = 12dB$

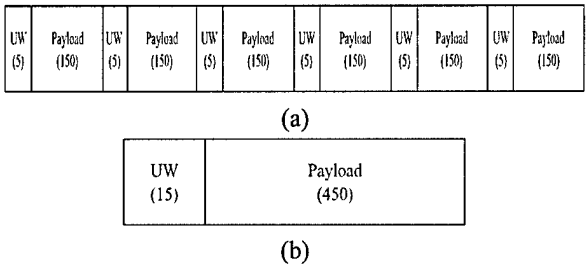


Fig. 5. Frame structure (in symbols) we used in our simulations. (a) Six-path SEEM, (b) Diversity with MRC.

and $f_d = 10Hz$. Observe that about $0.8dB$ gain can be achieved at $BER = 0.4\%$ and more than $1.3dB$ gain can be achieved at $BER = 0.3\%$. In Fig. 6b, we summarized the average bit error rate (BER) versus E_b/N_0 for Rician fading channel $K = 9dB$ and $f_d = 20Hz$. Observe that about $0.5dB$ gain can be achieved at $BER = 0.4\%$ and more than $1dB$ gain can be achieved at $BER = 0.3\%$.

C. Performance Analysis

Why our SEEM scheme can perform very well even with high probability (1%) to be compromised in each path? This can be explained based on the successful example of puncturing. Puncturing is often used to generate additional rates from a single convolutional code [2][5]. The basic idea behind puncturing is not to transmit some of the bits output by the convolutional encoder, thus increase the rate of the code. This increase in rate decrease the free distance of the code, but usually the resulting free distance is very close to the optimum one. The receiver inserts dummy bits to replace the punctured bits in the receiver, hence only one encoder/decoder pair is needed to generate several different code rates. In our M-path routing, a compromised path provides random values to the receiver node, and the receiver node de-interleaves the soft-decision output from demodulator (random value), which is very similar that some dummy bits are used to replace the bits from compromised path. But in our scheme, the effective puncturing pattern in terms of the number of bits and puncture location is time-varying from frame to frame.

V. Conclusions

We have proposed a SEEM aided with channel coding and interleaver scheme for wireless sensor networks. The M-path in multipath routing are selected using existing routing algorithm and fuzzy logic system considering the average remaining battery capacity and mobility of associated nodes. Simulation results show that our scheme performs much better than the diversity with MRC scheme in terms of BER. Our SEEM can tolerate some compromised nodes, which makes wireless sensor networks survivable

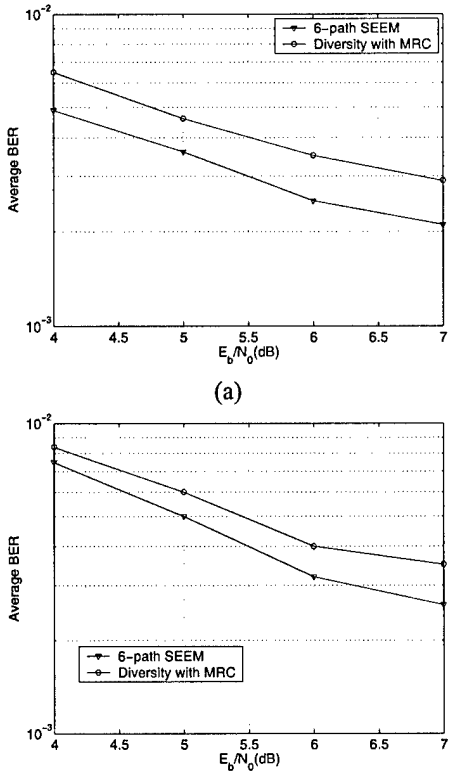


Fig. 6. Average BER versus E_b/N_0 for six-path SEEM and diversity with MRC in Rician fading channels (a) $K = 12dB$ and $f_d = 10Hz$, and (b) $K = 9dB$ and $f_d = 20Hz$.

and resilient because threat coming from compromised nodes is very difficult to detect.

ACKNOWLEDGEMENT

This work was supported by the U.S. Office of Naval Research (ONR) Young Investigator Program Award under Grant N00014-03-1-0466.

REFERENCES

[1] C. P. Bhagwat, "Highly dynamic destination-sequenced distance vector routing," *Proc. of ACM SIGCOMM'94*, pp.234-244, Sept 1994.

[2] J. B. Cain, G. C. Clark Jr, and J. M. Geist, "Punctured convolutional codes of rate (n-1)/n and simplified maximum likelihood decoding," *IEEE Trans on Information Theory*, vol. 25, pp. 97-100, Jan 1979.

[3] C. -C. Chiang, et al, "Routing in clustered multihop mobile wireless networks with fading channel," *Proc. IEEE Singapore Intl Conference on Networks*, 1997.

[4] J. Deng, R. Han, S. Mishra, "A Performance Evaluation of Intrusion-Tolerant Routing in Wireless Sensor Networks," *IPSN 2003*.

[5] J. Hagenauer "Rate compatible punctured convolutional codes and their applications," *IEEE Trans on Communications*, vol. 36, pp. 389-400, April 1988.

[6] W. C. Jakes, *Microwave Mobile Communication*, New York, NY: IEEE Press, 1993.

[7] D. Johnson and D. Maltz, *Mobile Computing*, Kluwer Academic Publishers, 1996.

[8] C. Karlof and D. Wagner, "Secure Routing in Sensor Networks: Attacks and Countermeasures," *SNPA 2003*.

[9] Y.W. Law, S. Dulman, S. Etalle and P. Havinga, "Assessing Security-Critical Energy-Efficient Sensor Networks," Department of Computer Science, University of Twente, Technical Report TR-CTIT-02-18, Jul 2002.

[10] S.J. Lee, and M. Gerla, " Split Multipath Routing with Maximally Disjoint Paths in Ad Hoc Networks ," *ICC 2001.*,

[11] Q. Li, J. Aslam, and D. Rus, "Online power-aware routing in wireless ad-hoc networks," *Proc. of Annual ACM/IEEE International Conf. on Mobile Computing and Networking (MobiCom)*, Rome, Italy, pp. 97-107, 2001.

[12] Q. Liang, "Optimal demodulator for satellite-based wireless ATM networks," *IEEE International Conference on Communications (ICC)*, May 2003, Alaska.

[13] J. M. Mendel, *Uncertain Rule-Based Fuzzy Logic Systems*, Prentice-Hall, Upper Saddle River, NJ, 2001.

[14] A. Nasipuri, and S.R. Das, " On-Demand Multipath Routing for Mobile Ad Hoc Networks ," *IEEE ICCCN 1999*, pp. 64-70.

[15] C. E. Perkins and E. Royer, "Ad hoc on demand distance vector routing," *Proc. 2nd IEEE Workshop o Mobile Computing Systems and Applications*, Feb 1999.

[16] J. G. Proakis, *Digital Communications (4nd Edition)* Kluwer AcMcGraw-Hill Higher Education, New York, 2001.

[17] S. Singh, M. Woo, and C. S. Raghavendra, "Power-aware routing in mobile ad hoc networks," *Proc. of Annual ACM/IEEE International Conf. on Mobile Computing and Networking (MobiCom)*, Dallas, TX, pp. 181-190, 1998.

[18] G. L. Stuber, *Principles of Mobile Communication (2nd Edition)* Kluwer Academic Press, 2001.

[19] A. Tsirigos, and Z.J. Haas, " Multipath routing in mobile ad hoc networks or how to route in the presence of frequent topology changes ," *IEEE MILCOM 2001*, pp. 878-883.

[20] L. Wang, Y.T. Shu, M. Dong, L.F. Zhang, and W.W. Yang, " Multipath Source Routing in wireless Ad Hoc Networks ," *Canadian Conference on Electrical and Computer Engineering*, vol. 1, pp. 479-483, 2000

[21] S. B. Wicker, *Error Control Systems for Digital Communication and Storage*, Prentice Hall, Upper Saddle River, NJ, 1995.

[22] Y. Xue and B. Li, "A location-aided power-aware routing protocol in mobile ad hoc networks," *Proc. of Globecom'2001*, pp. 2837-2841, San Antonio, TX, Sept 2001.

[23] L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks", *IEEE Networks, Special Issue on Network Security*, Nov/Dec 1999.

Energy and Mobility Aware Geographical Multipath Routing for Wireless Sensor Networks

Qilian Liang and Qingchun Ren
Department of Electrical Engineering
University of Texas at Arlington
Arlington, TX 76019-0016 USA
E-mail: liang@uta.edu, ren@wcn.uta.edu

Abstract— **In this paper, we propose an energy and mobility aware geographical multipath routing for wireless sensor networks. The remaining battery capacity, mobility, and distance to the destination location of candidate sensors in the local communication range are taken into consideration for next hop relay node selection, and a fuzzy logic system is applied to the decision making. Simulation results show that this scheme can extend the network lifetime longer than the original geographical routing scheme which only considers distance to the destination location, and this scheme can reduce the frame loss rate and link failure rate since mobility is considered.**

Index Terms : Wireless sensor networks, geographical routing, energy efficiency, fuzzy logic systems, mobility, channel fading.

I. Introduction

Wireless sensor networking is an emerging technology that promises unprecedented ability to monitor and manipulate the physical world via a network of densely distributed wireless sensor nodes. The nodes can sense the physical environment in a variety of modalities, including acoustic, video, seismic, thermal, and infrared, etc. In wireless sensor networks, there exists some challenges, for example,

- The routing path (link) failure may happen during data transmission because of collision, node dying out (no battery), node busy, or other accidents. Some applications require real time information and data, which means re-transmission is not possible. This motivates us to design a *multipath* routing scheme for wireless sensor networks.
- There exists energy constraint in wireless sensor networks because most sensors are battery operated. This motivates us to consider *energy* aware routing.
- Sensor mobility may cause the existing point-to-point route invalid before another route must be chosen. In physical layer, sensor mobility generates channel fading during data transmission, which degrades the performance in terms of bit error rate (BER) and frame error rate (FER). This motivate us to investigate a *mobility* aware routing.

In this paper, we propose an Energy and Mobility-aware Geographical Multipath Routing (EM-GMR) scheme for wireless sensor networks, and compare with Geographical Multipath Routing (GMR) scheme.

Many routing protocols have been developed for ad hoc networks, which can be summarized as two categories: table-driven (e.g., destination sequenced distance vector [1], cluster switch gateway routing [3]) and source-initiated on-demand-driven (e.g., ad hoc on-demand distance vector routing [15], dynamic source routing [8]). In [11], Lee and Gerla proposed a Split Multipath Routing protocol that builds maximal disjoint paths, where data traffic is distributed in two roots per session to avoid congestion and to use network resources efficiently. A Multipath Source Routing (MSR) scheme was proposed in [18], which is an extension of Dynamic Source Routing (DSR). Their work focuses on distributing load adaptively among several paths. Nasipuri and Das [14] presented the On-Demand Multipath Routing scheme, which is also an extension of DSR. In their scheme, alternative routes are maintained, which can be utilized when the primary one fails. Tsirigos and Haas [16] proposed a multipath routing scheme based on Diversity Coding. Three different paths are utilized to distribute the data, and x-for-y Diversity Coding is used to offer protection against at most x lost blocks out of the total $x + y$ blocks.

In sensor networks, location is more important than a specific node's ID. For example, in sensor networks for target tracking, where a target is located is much more important than the ID of reporting node. Therefore, some location-aware routing schemes have been proposed for wireless sensor networks. A greedy geographic forwarding with limited flooding to circumvent the voids inside the network was proposed in [4], and some properties of greedy geographic routing algorithms were studied in [19]. Jain et al[6] proposed a geographical routing using partial information for wireless sensor networks.

The rest of the paper is organized as follows. In Section II, we provde some preliminary knowleges on fuzzy logic system. In Section III, we present an energy and mobility-aware geographical multipath routing in a wireless sensor network. The simulation results and performance analysis are presented in Section IV, and in Section V, we conclude this paper.

II. Preliminaries: Overview of Fuzzy Logic Systems

Figure 1 shows the structure of a fuzzy logic system (FLS) [12]. When an input is applied to a FLS, the inference engine computes the output set corresponding to each rule. The defuzzifer then computes a crisp output from these rule output sets. Consider a p-input 1-output FLS, using singleton fuzzification, *center-of-sets* defuzzification [13] and "IF-THEN" rules of the form

$$R^l : \text{IF } x_1 \text{ is } \mathrm{F}_1^l \text{ and } x_2 \text{ is } \mathrm{F}_2^l \text{ and } \cdots \text{ and } x_p \text{ is } \mathrm{F}_p^l, \text{ THEN } y \text{ is } \mathrm{G}^l.$$

Assuming singleton fuzzification, when an input $\mathbf{x}' = \{x_1', \ldots, x_p'\}$ is applied, the degree of firing corresponding to the lth rule is computed as

$$\mu_{\mathrm{F}_1^l}(x_1') \star \mu_{\mathrm{F}_2^l}(x_2') \star \cdots \star \mu_{\mathrm{F}_p^l}(x_p') = \mathcal{T}_{i=1}^{p} \mu_{\mathrm{F}_i^l}(x_i') \quad (1)$$

where $\star$ and $\mathcal{T}$ both indicate the chosen t-norm. There are many kinds of defuzzifiers. In this paper, we focus, for illustrative purposes, on the center-of-sets defuzzifier [13]. It computes a crisp output for the FLS by first computing the centroid, c_{G^l}, of every consequent set G^l, and, then computing a weighted average of these centroids. The weight corresponding to the lth rule consequent centroid is the degree of firing associated with the lth rule, $\mathcal{T}_{i=1}^{p} \mu_{\mathrm{F}_i^l}(x_i')$, so that

$$y_{cos}(\mathbf{x}') = \frac{\sum_{l=1}^{M} c_{\mathrm{G}^l} \mathcal{T}_{i=1}^{p} \mu_{\mathrm{F}_i^l}(x_i')}{\sum_{l=1}^{M} \mathcal{T}_{i=1}^{p} \mu_{\mathrm{F}_i^l}(x_i')} \quad (2)$$

where M is the number of rules in the FLS.

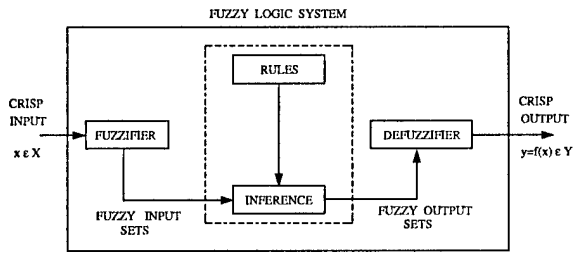


Fig. 1. The structure of a fuzzy logic system.

III. Energy and Mobility-aware Geographical Multipath-routing (EM-GMR)

In this paper, we propose an Energy and Mobility-aware Geographical Multipath Routing (EM-GMR) scheme. In the existing geographical routing approach (e.g., [6]), the path selection doesn't consider the remaining battery capacity of each node and its mobility, which are two very important factors for energy efficiency and network lifetime. Sensor mobility means the degree of channel fading, and high mobility requires higher signal-to-noise ratio for operating if the bit-error-rate (BER) or frame-error-rate (FER) requirements are given. In our EM-GMR, we consider *distance to the sensor node*, *remaining battery capacity*, and *mobility* of each sensor node. The geographical location of destination is known to the source node (as in [6]), and the physical location of each sensor node can be estimated easily if the locations of three sensor nodes (within a communication range) are known in wireless sensor network. Our scheme is a fully distributed approach where each sensor only needs the above three parameters, and we use fuzzy logic systems to handle these three parameters in the EM-GMR.

A. FLS for Node Selection in Multipath Routing

In this paper, we assume that each sensor node keeps a table which has some information about its neighbor nodes: locations, battery level, and mobility. The table is updated periodically by the locally-broadcasted information (beacon) from each neighbor node. The structure of a beacon is summarized in Fig. 2. We define a new term, *coherence time*, during which the three parameters (locations, battery level, and mobility) do not change very much. Coherence time is the shortest time duration that a sensor node will send another beacon. Each sensor examines itself the status of the three parameters in every coherence time period, and if a certain parameter has changed above a threshold, it will locally broadcast a beacon.

Type	Self Node ID	Position_X	Position_Y	Energy	Mobility

Fig. 2. Structure of a beacon.

There are one control channel and one data traffic channel in the sensor network. Direct sequence code-division multiple access (DS-CDMA) is used, and 64-bit Walsh sequence are used as speading sequence. The control channel is a common channel which means every node in its local communication range is able to obtain the message, and all 0's Walsh sequence is reserved for control channel. Each source node randomly generates M 64-bit Walsh sequences, and a spreading sequence is used

for each path. The spreading sequence is relayed to the next hop node via common control channel.

In our EM-GMR for M-path routing, the source node select M nodes in its communication range for the first hop relay. Assume there are N ($N > M$) nodes in its communication range, nodes who are further to the destination node than the source node are not considered. Choosing M nodes from remaining eligible nodes is based on a FLS (as will be described in detail). Starting the second hop, each node in the M-path selects its next hop node also using a FLS.

In our FLS design, we set up fuzzy rules for node selection based on the following three descriptors:

1) distance of a node to the destination,
2) its remaining battery capacity, and
3) its degree of mobility.

The linguistic variables used to represent the distance of a node to the destination were divided into three levels: *near*, *moderate*, and *far*; and those to represent its remaining battery capacity and degree of mobility were divided into three levels: *low*, *moderate*, and *high*. The consequent – the possibility that this node will be selected – was divided into 5 levels, *Very Strong, Strong, Medium, Weak, Very Weak*. So we need to set up $3^3 = 27$ (because every antecedent has 3 fuzzy sub-sets, and there are 3 antecedents) rules for this FLS.

A desired node to be included into the path should have near distance to the destination, high remaining battery capacity (so that the network life can last longer), and low mobility (so that channel fading will not be severe). Based on this fact, we design a fuzzy logic system using rules summarized in Table I.

We used trapezoidal membership functions (MFs) to represent *near*, *low*, *far*, and *high*, and triangle MFs to represent *moderate*. We show these MFs in Fig. 3a.

For every input (x_1, x_2, x_3), the output is computed using

$$y(x_1, x_2, x_3) = \frac{\sum_{l=1}^{27} \mu_{\mathrm{F}_l^1}(x_1)\mu_{\mathrm{F}_l^2}(x_2)\mu_{\mathrm{F}_l^3}(x_3)c^l}{\sum_{l=1}^{27} \mu_{\mathrm{F}_l^1}(x_1)\mu_{\mathrm{F}_l^2}(x_2)\mu_{\mathrm{F}_l^3}(x_3)} \quad (3)$$

where c^l is the centroid of consequent set. The output from FLS is degree of the possibility that this node will be selected into the path.

Our EM-GMR scheme consists of route discovery phase, route reconstruction phase, and route deletion phase. In the route discovery phase, the source node uses a FLS to evaluate all eligible nodes (closer to the destination location) in its communication range based on the parameters of each node: distance to the destination, remaining battery capacity, and degree of mobility. The source node chooses the top M nodes based on the degree of the possibility (output of FLS) that this node will be selected. The source node sends a Route Notification (RN) packet

TABLE I

THE RULES FOR NODE SELECTION IN MULTIPATH ROUTING. ANTECEDENT 1 (ANTE 1) IS *distance of a node to the destination*, ANTECEDENT 2 (ANTE 2) IS *its remaining battery capacity*, ANTECEDENT 3 (ANTE 3) IS *its degree of mobility*, AND CONSEQUENT IS *the possibility that this node will be included into the path.*

rule #	Ante 1	Ante 2	Ante 3	Consequent
1	near	low	low	medium
2	near	low	moderate	weak
3	near	low	high	very weak
4	near	moderate	low	medium
5	near	moderate	moderate	strong
6	near	moderate	high	weak
7	near	high	low	very strong
8	near	high	moderate	strong
9	near	high	high	medium
10	moderate	low	low	weak
11	moderate	low	moderate	very weak
12	moderate	low	high	very weak
13	moderate	moderate	low	medium
14	moderate	moderate	moderate	medium
15	moderate	moderate	high	weak
16	moderate	high	low	strong
17	moderate	high	moderate	strong
18	moderate	high	high	weak
19	far	low	low	weak
20	far	low	moderate	very weak
21	far	low	high	very weak
22	far	moderate	low	weak
23	far	moderate	moderate	weak
24	far	moderate	high	very weak
25	far	high	low	medium
26	far	high	moderate	strong
27	far	high	high	medium

to each desired node, and each desired node will reply using a REPLY packet if it is available. The structure of RN and REPLY is summarized in Fig. 4. If after a certain period of time, the source node did not receive REPLY from some desired node, it will pick the node with the $M+1$st degree of selection possibility. In the second hop, the selected node in each path will choose its next hop node uses a FLS. As illustrated in Fig. 5, node B needs to choose one node from eligible nodes C, D, E, F, H based on their three parameters, and sends RN packet to the selected node and waits for REPLY. If the top one node is unavailable (selected by another path or busy), then the top second node will be selected. By this means, M paths can be set up.

Each node is mobile, it may be possible that some node moves out of the communication range or some node dies out, which will lead to link failure, then a route reconstruction phase is started. The node immediately before the failure node in the routing path will apply FLS to determine the selection possiblity for all its eligible neighbor nodes, and choose the top one degree node (via RN-REPLAY procedure). The new node will determine its next

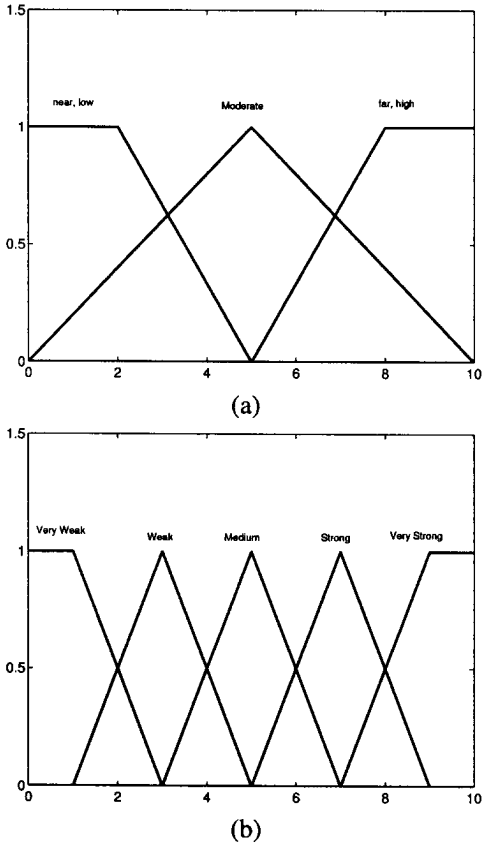


Fig. 3. The MFs used to represent the linguistic labels. (a) MFs for antecedents, and (b) MFs for consequent.

Type	Desired Node ID	Self Node ID	Dest_X	Dest_Y	Src_ID

Fig. 4. RN and REPLY packet structure.

node accordingly. Based on the source ID and destination location information in RN, it is easy to reconstruct the partial path failure.

The energy, mobility, and physical location of each node are changing. It may be possible that a node (in path) observes that its next node is not the optimal after a while, then this node will initiate a route deletion phase. This node will send an RN packet to the optimal node via common control channel, and this RN packet will also be received by the original relay node who will notice that the original path is deleted.

IV. Simulations and Performance Analysis

We ran our simulations using OPNET. 59 sensors were deployed randomly in an area with size $10km \times 10km$, and communication range (radius) was $1k$. Totally 59 sensors were deployed initially. The source and destination sensors

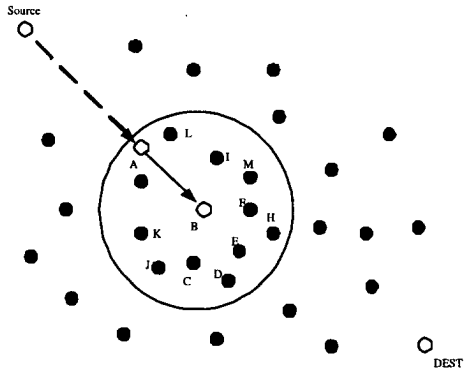


Fig. 5. Illustration of node selection.

were set with 2J initially, and 5 couples of source and destination nodes were communicating at the same time in this network. All the other sensors had intial energy from 0-2J. Each node (including source and destination nodes) had moving speed ranging from 0–10m/s. and its moving speed changed in every 10s, The frame length was 512 symbol and symbol rate was 9.6ksym/sec in our simulation.

Each sensor locally broadcasted a beacon message in every 2s to keep link, so that neighbor table could be updated (including new neighbor joins in, and old neighbors expire). These information are used for route discovery, reconstruction, and deletion. The coherence time were set as 10s in our simulation.

We used the same energy consumption model as in [5] for the radio hardware energy dissipation where the transmitter dissipates energy to run the radio electonics and the power amplifier, and the receiver dissipates energy to run the radio electronics. We chose the path-loss exponent $p = 2$. To transmit an l-symbol message a distance d, the radio expends:

$$E_{Tx}(l,d) = E_{Tx-elec}(l) + E_{Tx-amp}(l,d) = lE_{elec} + l\epsilon d^2 \quad (4)$$

and to receive this message, the radio expends

$$E_{Rx}(l) = E_{Rx-elec}(l) = lE_{elec} \quad (5)$$

The electronics energy, E_{elec}, as described in [5], depends on factors such as coding, modulation, pulse-shaping and matched filtering; and the amplifier energy, ϵd^2 depends on the distance to the receiver and the acceptable bit error rate. In this paper, we chose: $E_{elec} = 50nJ/sym$, $\epsilon = 10pJ/sym/m^2$. Same as [5][17], the energy for data aggregation is set as $E_{DA} = 5nJ/sym/signal$.

We compared our EM-GMR against the geographical multipath routing (GMR) scheme where only distance to the destination is considered. In Fig. 6, we plotted the simulation time versus the number of nodes dead. Observe that when 50% nodes (30 nodes) die out, the network

lifetime for EM-GMR has been extended about $\frac{175-125}{125} = 40\%$. In Fig. 7, we compared the frame loss rate of these two scheme. Observe that our EM-GMR outperforms the GMR for about 20% less frame loss. The average latency during transmission (end-to-end) is 419.68ms for our EM-GMR and 407.5ms for GMR, and link failure rate for EM-GMR is 5.68%, but for GMR is 10.42%.

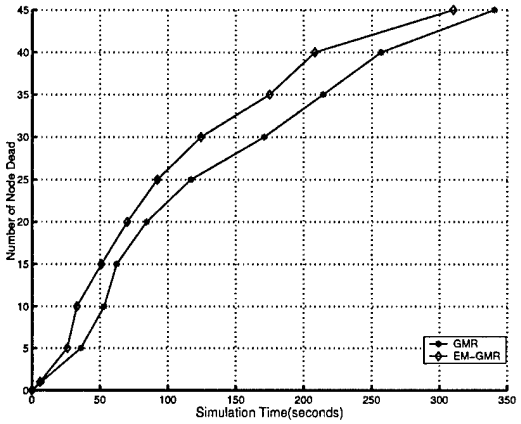


Fig. 6. Simulation time versus number of nodes dead.

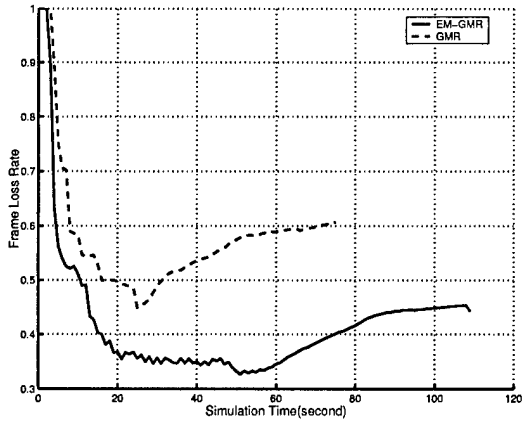


Fig. 7. Simulation time versus frame loss rate.

V. Conclusions

We have propose an energy and mobility aware geographical multipath routing for wireless sensor networks. The remaining battery capacity, mobility, and distance to the destination node of candidate sensors in the local communication range were taken into consideration for next hop relay node selection, and a fuzzy logic system was applied to the decision making. Simulation results showed that this scheme could extend the network lifetime about 40% comparing to the GMR scheme where only distance to the destination was considered. Besides, this scheme could tremendously reduce the frame loss rate and link failure rate since mobility was considered.

Acknowledgement

This work was supported by the U.S. Office of Naval Research (ONR) Young Investigator Program Award under Grant N00014-03-1-0466.

References

[1] C. P. Bhagwat, "Highly dynamic destination-sequenced distance vector routing," *Proc. of ACM SIGCOMM'94*, pp.234-244, Sept 1994.

[2] J. B. Cain, G. C. Clark Jr, and J. M. Geist, "Punctured convolutional codes of rate (n-1)/n and simplified maximum likelihood decoding," *IEEE Trans on Information Theory*, vol. 25, pp. 97-100, Jan 1979.

[3] C. -C. Chiang, et al, "Routing in clustered multihop mobile wireless networks with fading channel," *Proc. IEEE Singapore Intl Conference on Networks*, 1997.

[4] G. G. Finn, "Routing and addressing problems in large metropolitan-scale internetworks," *USC ISI Report ISI/RR-87-180*, March 1987.

[5] W. B. Heinzelman, et al, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Trans on Wireless Communications*, vol. 1, no. 4, pp. 660-670, Oct 2002.

[6] R. Jain, A. Puri, and R. Sengupta, "Geographical routing using partial information for wireless sensor networks," *IEEE Personal Communications*, pp. 48-57, Feb 2001.

[7] W. C. Jakes, *Microwave Mobile Communication*, New York, NY: IEEE Press, 1993.

[8] D. Johnson and D. Maltz, *Mobile Computing*, Kluwer Academic Publishers, 1996.

[9] C. Karlof and D. Wagner, "Secure Routing in Sensor Networks: Attacks and Countermeasures," *SNPA 2003*.

[10] Y.W. Law, S. Dulman, S. Etalle and P. Havinga, "Assessing Security-Critical Energy-Efficient Sensor Networks," Department of Computer Science, University of Twente, Technical Report TR-CTIT-02-18, Jul 2002.

[11] S.J. Lee, and M. Gerla, " Split Multipath Routing with Maximally Disjoint Paths in Ad Hoc Networks ," *ICC 2001.*,

[12] J. M. Mendel, "Fuzzy Logic Systems for Engineering : A Tutorial," *Proceedings of the IEEE*, vol. 83, no. 3, pp. 345-377, March 1995.

[13] J. M. Mendel, *Uncertain Rule-Based Fuzzy Logic Systems*, Prentice-Hall, Upper Saddle River, NJ, 2001.

[14] A. Nasipuri, and S.R. Das, " On-Demand Multipath Routing for Mobile Ad Hoc Networks ," *IEEE ICCCN 1999*, pp. 64-70.

[15] C. E. Perkins and E. Royer, "Ad hoc on demand distance vector routing," *Proc. 2nd IEEE Workshop o Mobile Computing Systems and Applications*, Feb 1999.

[16] A. Tsirigos, and Z.J. Haas, " Multipath routing in mobile ad hoc networks or how to route in the presence of frequent topology changes ," *IEEE MILCOM 2001*, pp. 878-883.

[17] A. Wang, et al, "Energy-scalable protocols for battery-operated microsensor networks," *Proc of IEEE Workshop on SIgnal Processing Systems (SiPS'99)*, Taipei, Taiwan, Oct 1999, pp. 483-492.

[18] L. Wang, Y. T. Shu, M. Dong, L.F. Zhang, and W.W. Yang, " Multipath Source Routing in wireless Ad Hoc Networks ," *Canadian Conference on Electrical and Computer Engineering*, vol. 1, pp. 479-483, 2000

[19] G. Xing, C. Lu, R. Pless, and Q. Huang, "On Greedy Geographic Routing Algorithms in Sensing-Covered Networks," *ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2004)*, Tokyo, Japan, May 2004.

DISTRIBUTED AND ENERGY EFFICIENT SELF-ORGANIZATION FOR ON-OFF WIRELESS SENSOR NETWORKS

Liang Zhao[1], Qilian Liang[2]

Department of Electrical Engineering, University of Texas at Arlington, Arlington, TX 76010, USA
[1]zhao@wcn.uta.edu, [2]liang@uta.edu

Abstract - In this paper, we utilize clustering to achieve energy efficiency for the on-off wireless sensor network, whose member nodes alternate between active and inactive states. In the proposed Distributed and Energy Efficient Self-Organization (DEESO) scheme, the head election is adjusted adaptively to the energy reserve of local active nodes. Furthermore, we apply the Adaptive Channel Assignment to address the on-off topology changes. Simulation results show that DEESO delivers 184% amount of data to the base station as LEACH for the same amount of dissipation and the effective network lifetime is extended around 56%.

Keywords - wireless sensor networks, energy efficiency, clustering

I. INTRODUCTION

A wireless sensor network can be thought of as an *ad hoc* network consisting of sensors linked by a wireless medium to perform distributed sensing tasks. Sensor networks share many communication technologies with *ad hoc* networks, but there are some vital differences such as dense deployment and energy constraint [1], thus the protocols developed for traditional wireless ad hoc networks are not necessarily well suited to the unique features of sensor networks. When a sensor node may have to operate for a relatively long duration on a tiny battery, energy efficiency becomes a major concern.

A variety of "power-aware" routing protocols have been proposed to address this problem. In one school of thoughts [2]–[4], the traditional Shortest Path First strategy is replaced by Least Energy First routing, i.e., a multihop route is preferred to a single-hop one if only multiple short-distance relays cost less energy than a single long-distance transmission. For example, "Minimum Transmission Energy"(MTE) routing [3], [4] was proposed in place of traditional "minimum hops routing". Another school of thoughts is that nodes are clustered so that a hierarchy is formed. LEACH (Low-Energy Adaptive Clustering Hierarchy) [5], an example of the latter school, can improve network lifetime by an order of magnitude compared with general-purpose multihop approaches, which is referred to as *clustering gain* in the following discussion.

This work was supported by the Office of Naval Research(ONR) Young Investigator Award under Grant N00014-03-1-0466.

Unfortunately, the network model on which LEACH is based is basically a static one, in which nodes are always on and have data to send to the base station. In fact, due to node mobility, shutdown or failure, topology changes are frequent in sensor networks, and LEACH suffers drastically in those cases. In this paper, we consider the topology changes due to sensors' alternating between active and inactive states and propose Distributed and Energy Efficient Self-Organization (DEESO) to address this problem.

The rest of this paper is organized as follows. We discuss the clustering criterion and present DEESO in Section II. Simulations are given in Section III and the results are discussed in Section IV. Section V concludes this paper.

II. DEESO

A. Lifetime Model

The Always-On model is used in [5], where the nodes are supposed to be always active and have data to transmit. In real applications, the nodes are often set to alternate between active and inactive states in order to save energy. And occasionally, the nodes may have no data for transmission, which can be regarded as inactive. Thus, the On-Off model may be a better approximation of the sensors' lifetime model [6], in which the active and inactive durations of nodes obey the exponential probability law with mean T_a and T_s respectively. Thus, the average number of active nodes is given by

$$E[N_a] = T_a/(T_a + T_s). \quad (1)$$

B. Channel Assignment

The term channel, in one of its narrow sense, means a band of frequency which is assigned to a user for exclusive usage. In wide sense, it could indicate a time slot or a spread spectrum code. To increase capacity and minimize interference, a variety of channel assignment strategies have been developed and can be classified into fixed, dynamic or adaptive. [7]

In a Fixed Channel Assignment strategy (FCA), each user is allocated a predetermined set of channels. Any transmission attempt can only succeed by the channel granted. If all the channels are occupied, no new user can access the channels. For example in LEACH, if a sensor activates in the middle of the round, it can not be accepted by any existing

cluster so that it has to communicated directly with the base station and lose the clustering gain. On the other hand, in Dynamic Channel Assignment strategy(DCA), channels are not allocated permanently, but assigned and released on request. DCA can make better use of channels while introducing more protocol overhead and channel management.

The trade-off is Adaptive Channel Assignment (ACA), in which a division of channels are assigned to current users in a fixed manner while the rest of channels are reserved for prospective users and will be assigned on demand. ACA not only moderates the waste of channels in FCA but also reduces protocol overhead and channel management.

C. Protocol Description

DEESO is especially designed for energy efficiency and higher tolerance to on-off topology changes. Unlike LEACH, it is a distributed self-organizing scheme without any central control or dependence on other routing schemes.

In DEESO, Direct Sequence Spread Spectrum is utilized for higher tolerance to interference, low detectability and multiple access communication by a large population of relatively uncoordinated users. Some Spread Spectrum codes may be set aside as public channels, and each cluster has its own Spread Spectrum code so that the interference between clusters is minimized. For intracluster communications, TDMA is used with Adaptive Channel Assignment (ACA). Specifically, when a cluster is formed, the clusterhead creates and broadcasts a time schedule to its member. As shown in Fig.1, each member is assigned a time slot per frame to send its data to the clusterhead, and the extra time slots are reserved for prospective members. For most applications for sensor networks, the traffic is relatively low [1] so that there is always enough free slots for reservation.

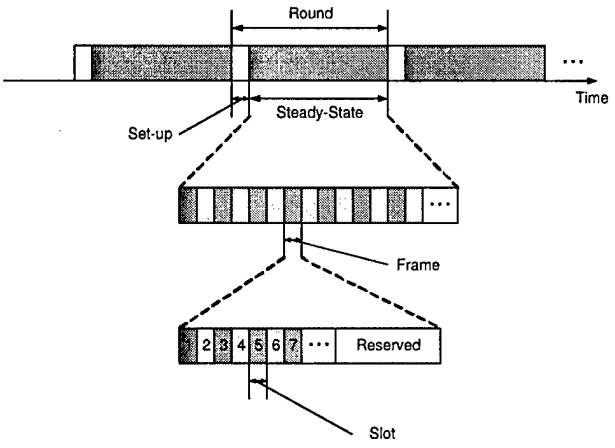


Fig. 1
Time line showing DEESO's frame structure.

The state transition diagram is shown in Fig.2. At the beginning of each round, all nodes start at the stand-alone state, broadcasting their vital information at the maximum output power level. Then based on the vital information, the strongest are elected as clusterheads and others join the closest cluster according to received signal strength. A non-head member may doze off according to its schedule. If a sensor node wakes up during the steady-state phase of a round, it eavesdrops the public channel for STANDY-BY duration. If it finds some nearby clusterheads, it will choose the one with strongest received signal strength as its clusterhead. Otherwise, it elects itself as clusterhead and starts recruiting other nodes. When the round ends, the nodes return to stand-alone state and a new round will begin.

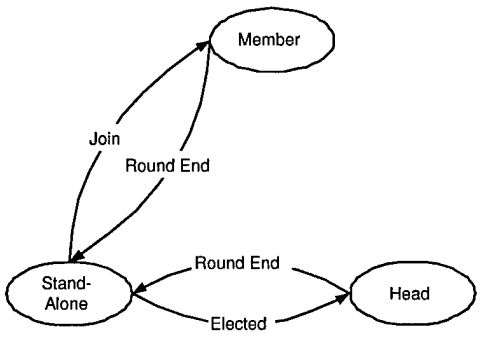


Fig. 2
State transition diagram of a node in DEESO

1) Information Exchange: The only vital information needed by DEESO is the battery level. The exchange of position information is not required because the distance between nodes can be can estimated by the received signal strength according to the path loss model given that the broadcast power level is known a priori. Unlike LEACH, the vital information exchange in DEESO is totally based on access, i.e., there is no routing or relaying of the vital information. Eventually, each node obtains its one-hope neighbor information. When a sensor node wakes up during the steady-state phase of a round, it can retrieve the neighbor lists from the nearby clusterheads.

2) Head Election: In LEACH, each node elects itself as clusterhead by the probability

$$p_{head}(i) = k\frac{E(i)}{E_{total}}, \tag{2}$$

where $E(i)$ is the i^{th} node's energy, E_{total} is the total energy and k is the optimal number of clusters. Since E_{total} is inaccessible to sensor nodes unless there is other routing schemes or central control available, LEACH is unable to determine the battery levels of active nodes in the whole network and thus has to base on the predetermined parameter N and average battery level. Although the average

number $E[N_a]$ of active nodes can be calculated by (1) in experiments, such estimation is impossible in real application as the average active and sleeping durations are unknown before the nodes are deployed to observe the phenomenon of interest.

In DEESO, the self-electing probability is determined by

$$p'_{head}(i) = k' \frac{E(i)}{E'_{total}}, \tag{3}$$

where E'_{total} is the total energy in the neighborhood. Since we use E'_{total} instead of E_{total}, k' will be different from k in (2). Since it is mathematically difficult to determine k or k' analytically, we ran simulations at different $k(k')$'s to determine the optimal one as shown in Section III.

3) Cluster Formation: Based on the received signal strength, each non-head node chooses the nearest clusterhead and send a "Request-to-join" message to the clusterhead. Then the clusterhead creates the time schedule in which time slots are allocated for intracluster communication, data aggregation, intercluster communication, maintenance and other possible usage.

4) Steady State: After the clusters are formed, the sensor network enters the steady-state phase. During the "intra-cluster slots", the clusterhead receives data from members; during the "data aggregation slots", it can turn off radio and perform data aggregation; and then it sends the resulting data back to the base station during the "intercluster slots"; it can broadcast advertisements and recruit new members during "maintenance slots".

III. Simulations

In this section, we compare the performance of DEESO and LEACH using computer simulations. 100 nodes with 2J initial energy were evenly distributed in a circular region with diameter of 100 m, and the base station was located at $(125m, 0)$. We ran 1000 simulations for each case and plotted received data and the number of survival nodes.

The following model is adopted from [5] where perfect power control is assumed. To transmit l bits over distance d, the sender's radio expends

$$E_{TX}(l,d) = \begin{cases} lE_{elec} + l\epsilon_{fs}d^2, & d < d_0 \\ lE_{elec} + l\epsilon_{mp}d^4, & d \geq d_0 \end{cases} \tag{4}$$

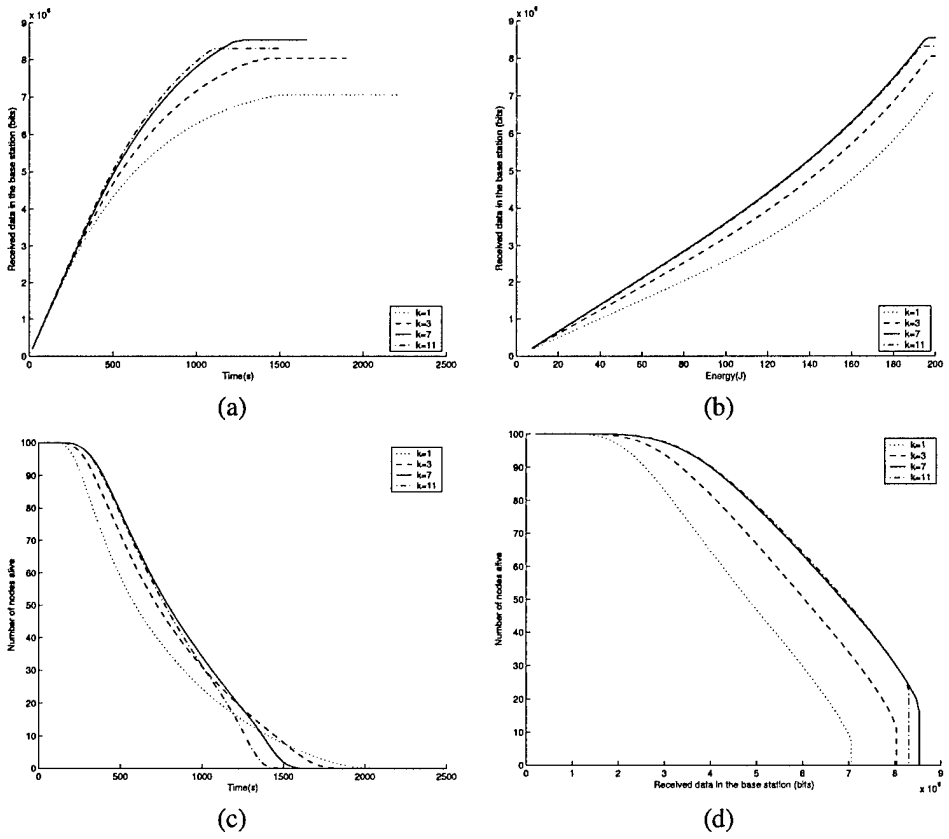


Fig. 3

Data of LEACH at varying k. (a) Amount of data received at the base station over time. (b) Amount of data received at the base station per given amount of energy. (c) Number of survival nodes over time. (d) Number of survival nodes per amount of data received in the base station.

and the receiver's radio expends

$$E_{RX}(l,d) = lE_{elec}. \quad (5)$$

And the communication energy parameters are set as in Table 1.

Table 1
Simulation Parameters

Name	Value
d_0	86.2m
E_{elec}	$50nJ/bit$
ϵ_{fs}	$10pJ/bit/m^2$
ϵ_{mp}	$0.0013pJ/bit/m^4$

A. Optimal k

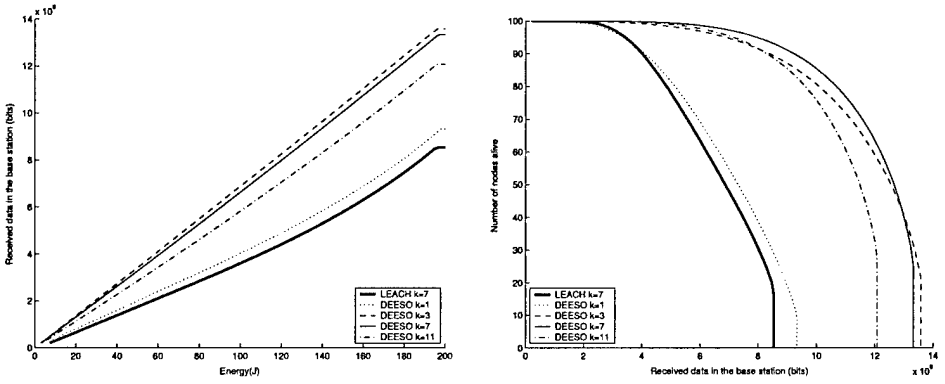
In this case, the effect of k on energy efficiency is evaluated. Fig.3(a)(b) shows the amount of data received at the base station over time and per given amount of energy. Fig.3(c)(d) shows the number of survival nodes over time and per amount of data received in the base station. Note that there exists a critical phase during which the survival nodes virtually send no data to the base station while they are still alive. The critical phase is indicated by a horizontal line in Fig.3(a) and a plunging line in Fig.3(d). The reason for the critical phase is that these nodes still try in vain to organize themselves into clusters but have no successful transmission. Thus, the effective lifetime, whose end is marked by the critical phase, is preferred to the actual lifetime as the benchmark. Taking $k = 1$ and $k = 7$ as examples, although Fig.3(c) shows a crossover between two curves, Fig.3(d) distinctly shows the the effective lifetime of $k = 7$ is far longer than that of $k = 1$. Fig.3 shows that the critical phase comes earlier when k is far away from 7. When k is nearly 7, the performances are virtually identical. This is due to the random head selection, which does not guarantee the given k clusterheads are selected. This could be an advantage for robusticity as it does not stick to a single fixed k.

B. LEACH vs DEESO

In this case, the performances of LEACH and DEESO are compared. Fig.4(a) clearly shows that DEESO delivers 184% amount of data to the base station as LEACH for the same amount of dissipation. The first reason for such improvement is DEESO's indenpence of other routing schemes. It can estimate the energy distibution of local active nodes by eavedropping the neighbors' vitial information. On the other hand, LEACH has to use the predetermined number of nodes if no other routing scheme is available to relay such information. The second reason is that Adaptive Channel Assignment is used in DEESO so that a node can be accecpted by the nearest clusterhead when it turns on during a round. The Fixed Channel Assignment in LEACH forbids the clusterhead to accept a new member on the run, and the newly woken-up node has to claim itself as the clusterhead, which is generally not energy efficient. Thanks to the energy efficiency demonstrated by DEESO, the effective network lifetime is extended by around 56% as shown in Fig.4(b).

IV. Discussion

The energy dissipation model we develop here is adopted from [5], where rectangle coordinates are utilized. Assume that there are N nodes distributed uniformly in a circular region with radius of R and a cluster algorithm divides nodes into k clusters, then there are approximately $n = N/k$ nodes



(a) (b)

Fig. 4
Data of LEACH and DEESO. (a) Amount of data received at the base station per given amount of energy. (b) Number of survival nodes per amount of data received in the base station. These graphs show that DEESO extends the effective network lifetime by 56% and delivers 184% amount of data to the base station as LEACH for the same amount of dissipation.

in each cluster. The power dissipated in the cluster head node is

$$\begin{aligned} E_{CH} &= lE_{elec}(n-1) + lnE_{DA} + l(E_{elec} + \epsilon_{mp} d_{toBS}^4 \quad (6) \\ &= lnE_{elec} + lnE_{DA} + l\epsilon_{mp} d_{toBS}^4) \end{aligned}$$

where l is the bits each sensor collects in a round, d_{toBS} is the distance from the cluster head node to the base station. And the energy used in each non-head node is

$$E_{non-CH} = lE_{elec} + l\epsilon_{fs} d_{toCH}^2 \quad (7)$$

where d_{toCH} is the distance from the non-head node to the corresponding head. Assume the area occupied by a cluster is circular and is approximately $\pi R^2/k$,then the cluster radius is

$$R_c = \frac{R}{\sqrt{k}}. \quad (8)$$

Assuming the node head is at the center of mass of the cluster,

$$\begin{aligned} E[d_{toCH}^2] &= \int\int r^2 \rho(r,\theta) r dr d\theta \\ &= \int_0^{2\pi} \int_0^{R_c} r^2 \rho(r,\theta) r dr d\theta \\ &= \frac{\pi \rho R^4}{2k^2} \quad (9) \end{aligned}$$

Substituting $\rho = 1/(\pi R_c^2) = k/\pi R^2$ into (9),

$$E[d_{toCH}^2] = \frac{R^2}{2k} \quad (10)$$

Therefore, the total power dissipated in each cluster is

$$\begin{aligned} E_{cluster} &= E_{CH} + (n-1)E_{non-CH} \\ &\approx E_{CH} + nE_{non-CH} \quad (11) \end{aligned}$$

and the total power dissipated in the whole network is

$$\begin{aligned} E_{total} &= kE_{cluster} \\ &= Nl\{E_{elec} + E_{DA} + \frac{1}{n}\epsilon_{mp} d_{toBS}^4 \\ &\quad + E_{elec} + \epsilon_{fs}\frac{R^2}{2k}\} \quad (12) \end{aligned}$$

The optimal value of k is found by letting $\frac{\partial E_{total}}{\partial k}$ to zero,

$$k^* = \sqrt{\frac{N\epsilon_{fs}}{2\epsilon_{mp}}} \frac{R}{d_{toBS}^2} \quad (13)$$

For our experiments, the base station is located at $(125m, \pi/2)$, then d_{toBS}^2 can be estimated by

$$\begin{aligned} E[d_{toBS}^2] &= \int\int |r - r_{BS}|^2 \rho(r,\theta) r dr d\theta \\ &= \frac{1}{\pi R^2} \int_0^{2\pi} \int_0^{R} (r^2 + r_{BS}^2 \\ &\quad - 2rr_{BS} cos(t - \pi/2)) r dr dt \quad (14) \\ &= 20625 \quad (15) \end{aligned}$$

By substituting (15) into (13), we obtain

$$k^* \approx 1.2 \quad (16)$$

This optimal value does not agree with $k_opt \approx 7$ obtained in our simulations(see Section III-A). The main reason for such difference is that the random head election used in both LEACH and DEESO can not guarantee the desired number of clusterheads be elected.

V. Conclusion

We utilize clustering to recognize the most energy efficient pattern in organizing the on-off wireless sensor nodes. On the basis of LEACH, we proposed DEESO to address the on-off topology changes. The adaptiveness of DEESO helps reducing the Communication-related Energy Dissipation to more than half. However, the random head election used in both LEACH and DEESO can not guarantee the desired number of clusterheads be elected. Whether such randomness could damage the energy efficiency is interesting for further study.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Commun. Mag.*, vol. 20, pp. 102–114, Aug. 2002.

[2] R. Min, M. Bhardwaj, S.-H. Cho, N. Ickes, E. Shih, A. Sinha, A. Wang, and A. Chandrakasan, "Energy-centric enabling technologies for wireless sensor networks," *IEEE Wireless Commun. Mag.*, vol. 9, pp. 28–39, Aug. 2002.

[3] T. Shepard, "A channel access scheme for large dense packet radio networks," in *Proc. ACM SIGCOMM*, Stanford, CA, Aug. 1996, pp. 219–230.

[4] M. Ettus, "System capacity, latency and power consumption in multihop-routed ss-cdma wireless networks," in *Proc. Radio and Wireless Conf. (RAWCON'98)*, Colorado Springs, CO, Aug. 1998, pp. 55–58.

[5] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Trans. Wireless Commun.*, vol. 1, no. 4, pp. 660 – 670, Oct. 2002.

[6] T.-C. Hou and T.-J. Tsai, "An access-based clustering protocol for multihop wireless ad hoc networks," *IEEE J. Select. Areas Commun.*, vol. 19, pp. 1201–1210, July 2001.

[7] T. S. Rappaport, *Wireless Communications:Principles and Practice*. Upper Saddle River, NJ: Prentice-Hall, 2002.

Energy-Efficient Self-Organization for Wireless Sensor Networks: A Fully Distributed Approach

Liang Zhao, Xiang Hong, Qilian Liang Department of Electrical Engineering
University of Texas at Arlington
Arlington, TX 76010, USA
Email: {zhao, hong}@wcn.uta.edu, liang@uta.edu

Abstract

In this paper, we utilize clustering to organize wireless sensors into an energy-efficient hierarchy. We propose an Expellant Self-Organization (ESO) scheme that uses expellant election to achieve local energy efficiency. This scheme is based on a new criterion which can be used by each sensor node to make a distributed decision on whether electing to be a cluster head or a nonhead member, which is a fully distributed approach. Although ESO uses only local information, it achieves better performance in terms of effective lifetime and Data/Energy Ratio compared with native LEACH which relies on other routing algorithms to access global information. A complementary exponential data correlation model is also introduced to simulate different data aggregation effect.

Index Terms : Wireless sensor networks, energy-aware systems, clustering, distributed applications

I. Introduction

A wireless sensor network (WSN) can be thought of as an *ad hoc* network consisting of sensors linked by a wireless medium to perform distributed sensing tasks. WSNs share many communication technologies with *ad hoc* networks, but there are some vital differences such as dense deployment and energy constraint [1], thus the protocols developed for traditional wireless ad hoc networks are not necessarily well suited to the unique features of WSNs. When a wireless

sensor may have to operate for a relatively long duration on a tiny battery, energy efficiency becomes a major concern.

A variety of "power-aware" routing protocols have been proposed to address this problem. In one school of thoughts [2]–[4], the traditional Shortest Path First strategy is replaced by Least Energy First routing, i.e., a multihop route is preferred to a single-hop one if only multiple short-distance relays cost less energy than a single long-distance transmission. For example, "Minimum Transmission Energy"(MTE) routing [3], [4] was proposed in place of traditional "minimum hops routing". Another school of thoughts is that nodes are clustered so that a hierarchy is formed. Based on the observations on cellular networks [5]–[13], [19], it would be advisable to partition nodes into clusters for the reasons such as spatial reuse, less update cost, less routing information and less data transmission.

Another dispute in previous *ad hoc* networks research is whether a cluster head be elected within each cluster. Some researchers [5], [9], [10] argue that it is unreasonable to have a cluster head because every node has similar energy constraint and the cluster head will consume energy much faster. Their methodology breaks the information exchange into two parts; cluster members proactively perform the intracluster exchange, and intercluster information exchange is achieved by demand-based operations. This approach does have some advantage when the traffic is mostly within the cluster, however, when the major traffic in WSN is directed from sensor nodes to the base station, i.e., of intercluster type, headless structure suffers from cumbersome intercluster information exchange.

On the other hand, the extra burden of cluster head can be mitigated by rotating the headship among the members. The rotation can also take advantage of the relaxation effect [17], which indicates frequently reducing the current drawn from the battery enables the battery to recover a portion of its lost capacity and hence lengthens the battery lifetime. In addition, the cluster head can perform data fusion and reduce the data sent back to the base station. LEACH (Low-Energy Adaptive Clustering Hierarchy) [16], an example of the latter school, can improve network lifetime by an order of magnitude compared with general-purpose multihop approaches. In conclusion, the characteristics of WSN prefer hierarchical structure with cluster heads.

However, the cluster formation in LEACH is based on global information. To access such information, other routing schemes are required. In this sense, LEACH is only a semi-distributed protocol for WSN. The other problem with LEACH is the random head election that can

not guarantee that the desired number of cluster heads be elected or the elected heads be evenly positioned. In this paper, we are concerned to optimize the cluster formation using only local information and propose an Expellant Self-Organization(ESO) scheme which uses a fully distributed approach.

The paper is organized as follows. Section II reviews LEACH and its radio energy consumption model. Section III introduces the data correlation model that our research is based on. In section IV, we make data-centric analysis of energy consumption in WSN and propose a new criterion which ESO bases the self-electing decision on. ESO is described in Section V and simulations are given in Section VI. Section VII concludes this paper.

II. Related Work

A. LEACH

Our energy-efficient clustering research is based on the hierarchy of LEACH which uses a CDMA-TDMA hybrid communication scheme. Each cluster has its own Spread Spectrum code so that the interference between clusters is minimized. For intracluster communications, TDMA slots are assigned by the cluster head to it members to minimize the competition for the shared wireless media. The operation of LEACH is divided into rounds. At the beginning of each round, cluster heads are elected and other nodes join them as members. When a cluster is formed, the cluster head creates and broadcasts a time schedule to its members. As shown in Fig. 1, each member is assigned a time slot per frame to send its data to its cluster head, and then the cluster head performs data aggregation and sends the resulting data back to the base station. Compared with multihop routing schemes, LEACH demonstrates outstanding energy efficiency, which is referred to as clustering energy gain in the following.

However, there are several drawbacks in LEACH's cluster formation:

a. **Dependence on global information** In LEACH, each node i elects itself to be a head at the beginning of round $r+1$(which starts at time t) with probability $P_i(t)$. Reference [16] provides two ways to determine the self-electing probability $P_i(t)$. If all nodes are assumed to start with an equal amount of energy, $P_i(t)$ is given by

$$P_i(t) = \begin{cases} \frac{c}{N - c*(r \bmod \frac{N}{c})} & : C_i(t) = 1 \\ 0 & : C_i(t) = 0 \end{cases}, \quad (1)$$

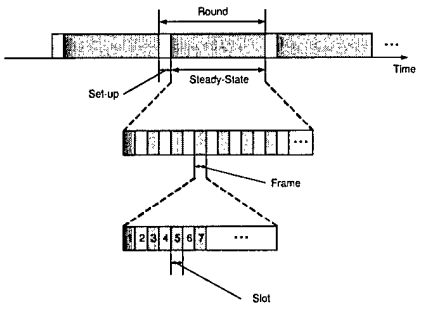


Fig. 1. Time line showing LEACH's frame structure.

where c is the desired number of clusters and $C_i(t)$ is the indicator function determining whether or not node i has been a head in the most recent $(r \ mod \ (N/c))$ rounds. The more general estimate of $P_i(t)$ is given by

$$P_i(t) = min\{\frac{E_i(t)}{E_{total}(t)}c, 1\}, \tag{2}$$

where $E_i(t)$ is the current energy(i.e. remaining battery capacity) of node i and

$$E_{total}(t) = \sum_{i=1}^{N} E_i(t). \tag{3}$$

Effectively, N in (1) and E_{total} in (2) are global information, which compromise the distributedness of LEACH.

b. **Random election** Although random decision often strengthens the robusticity by avoiding sticking to a single choice, too much randomness may shift the decision away from the optimal range. In LEACH's case, suppose (2) is used and all nodes have equal amount of energy, if N nodes want to elect c heads among them, then the self-electing probability for each node is

$$p = \frac{c}{N} \tag{4}$$

Then the probability of "n heads are elected" is

$$Pr(n \text{ elected heads}) = \binom{N}{n} p^n (1-p)^{(N-n)} \tag{5}$$

The distribution of the number of elected heads is listed in Table I. Obviously, too few (Fig. 2(c)) and too many (Fig. 2(d)) elected heads would damage the energy efficiency.

Moreover, in the case of "no elected head" whose probability listed in row 1, all the nodes have to communicate directly with the base station, in which case all the clustering energy gain is lost. When the number of elected heads is too few, for example, only one head is elected, the head may be exhausted by the tremendous data sent to it. In such cases, the energy efficiency is tremendously compromised.

TABLE I

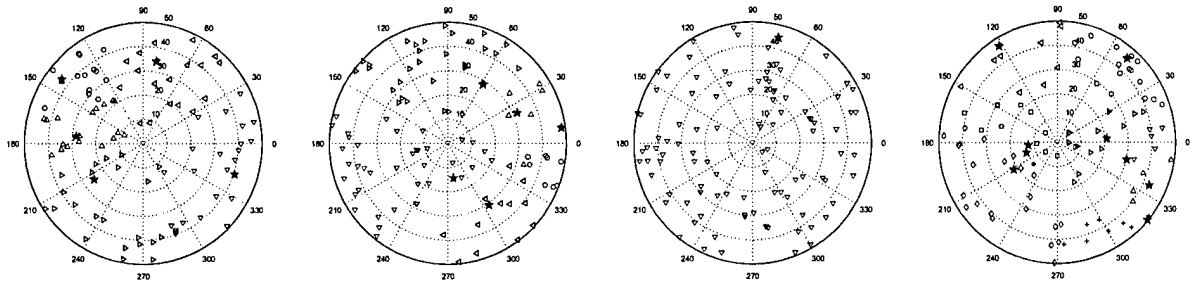
OUTCOME OF 100 NODES ELECTING 5 HEADS.

n: number of elected heads	$Pr(n$ elected heads)
0	0.0059
1	0.0312
2	0.0812
3	0.1396
4	0.1781
5	0.1800
6	0.1500
7	0.1060
8	0.0649
9	0.0349
≥ 10	0.0341

Another problem introduced by the random head selection is that the positions are not taken into consideration. Obviously, the even layout of heads would favor energy efficiency. When heads are randomly selected as in LEACH, elected heads sometimes clump together (Fig.2(b)), which leads to unnecessary energy waste.

B. Radio Energy consumption

According to the path loss model [19], the energy E required to transmit over distance d is given by $E \sim d^{\beta}$, where β is the pass loss exponent, whose value depends on the specific propagation environment. For example, β will have a larger value for long distance transmission than for short distance transmission. To save energy and reduce interference, the power control is widely utilized in wireless communications [19] so that the radio is adjusted for a range of output power level.



(a) (b) (c) (d)

Fig. 2. 100 nodes elect 5 heads (Heads marked by pentagrams). (a) Five heads are elected and evenly distributed. (b) Five heads are elected and clump in the right semicircle. (c) Only one head is elected. (d) Nine heads are elected.

The following model is adopted from [16] where perfect power control is assumed. To transmit l bits over distance d, the sender's radio expends

$$E_{TX}(l,d) = \begin{cases} lE_{elec} + l\epsilon_{fs}d^2 & d < d_0 \\ lE_{elec} + l\epsilon_{mp}d^4 & d \geq d_0 \end{cases} \tag{6}$$

and the receiver's radio expends

$$E_{RX}(l,d) = lE_{elec}. \tag{7}$$

And the communication energy parameters are set as
d_0=86.2m, E_{elec}=$50nJ/bit$, ϵ_{fs}=$10pJ/bit/m^2$, ϵ_{mp}=$0.0013pJ/bit/m^4$.

III. Data Correlation Model

The data collected by neighboring sensors have a lot of redundancy, thus, [16] assumes perfect data correlation that all individual signals from members of the same cluster can be combined into a single representative signal. Nevertheless, this assumption can not hold when the cluster size increases to some extent. Therefore, we develop a complementary exponential data correlation model and use it in evaluating energy consumption.

Considering the phenomenon of interest as a random process, the correlation between data collected by two sensors is generally a decreasing function of the distance r between them. After the data aggregation removes most of the redundancy, the residue can be assumed to be an

increasing function of r. Based on the above observation, the data aggregation effect is modeled as below.

Suppose there are M_k nonhead members in cluster k ($k = 1, 2, 3, ..., c$), the ith member ($i = 1, 2, 3, ..., M_k$) collects l bits and sends them back to its head k at distance r_{ki}, the head expends $2lE_{DA}$ Joules on the data aggregation of the $2l$ bits (l bits collected by itself and another l bits by its ith member), where E_{DA} is set as $5nJ/bit$ as in [16]. The resulting data is assumed of $l(1+\eta_{ki})$ bits, where η_{ki} is data aggregation residue ratio and assumed to be complementary exponential, namely,

$$\eta_{ki} = 1 - e^{-\alpha r_{ki}}. \tag{8}$$

Then, the resulting data from the whole cluster k is

$$l(1 + \sum_{i=1}^{M_k} \eta_{ki}) \tag{9}$$

α is a small positive real number whose magnitude depends on specific phenomenon of interest. For example, the photic, acoustic, seismic and thermal signals often show a strong correlation at short distance, and thus, α will have smaller values for such data. Since η is a monotonously decreasing function of α and r, η approaches zero for smaller α and r. This model can approach the perfect-data-correlation assumption in [16] by decreasing α or approach the no-data-aggregation assumption in [3], [4] by increasing α, thus, different scenarios can easily be set up by varying α.

IV. Optimal Clustering

In this section, we make data-centric analysis of energy consumption in WSN and propose a new criterion which is the theoretical basis of ESO.

A. Problem Formulation

Clustering has been widely used in pattern recognition, and we use it to obtain the energy-efficient organization for WSN. From the data-centric view, the data collected by a node can be sent back directly to the base station or relayed by a cluster head. The first case occurs if this node is a cluster head; the data collected by head k is data-aggregated (with the data collected

by its members) and sent back to the base station. Thus, the energy cost for each bit of data collected by head k is

$$J_{CH(k)} = E_{DA} + E_{elec} + \epsilon_{mp} d_k^4, \tag{10}$$

where d_k is the distance between head k and the base station.

For the second case, consider nonhead member ki with its head k at the distance r_{ki}, member ki sends its data to head k, and then head k performs data aggregation on the data and sends the resulting data to the base station. Thus, the energy cost for each bit of data collected by nonhead member ki is

$$J_{CM(ki)} = E_{elec} + \epsilon_{fs} r_{ki}^2 + E_{elec} + E_{DA} + \eta(r_{ki})(E_{elec} + \epsilon_{mp} d_k^4). \tag{11}$$

Considering all c clusters, the overall cost is

$$J_{total} = \sum_{k=1}^{c} \{J_{CH(k)} + \sum_{i=1}^{M_k} J_{CM(ki)}\}, \tag{12}$$

where M_k is the number of nonhead members in cluster k.

Taking $E[J_{total}]$ the expected value of the overall energy cost as the objective function, the original problem is translated into an objective function clustering [20]. If a central control scheme is possible, an iterative algorithm can be run at the base station to minimized $E[J_{total}]$. For example, Fuzzy c-Means is utilized in [18] to minimize an Euclidean-distance-based functional representing the energy cost in Wireless Personal Area Networks. However, since WSNs are working in *ad hoc* mode, clustering decision must be distributed to each sensor node. Thus, our goal is using only local information to achieve energy-efficient clustering.

B. Benefit Range

Generally, if a node is close to a cluster head, there is some energy gain if it joins that cluster. The energy gain diminishes when the distance between the nonhead member and the head increases. Consequently, the energy gain approaches zero at some critical distance, termed as benefit range. To determine the benefit range, consider a node with a head at distance r. The node could choose to be a nonhead member or a head, which would consequently cost J_{CM} or J_{CH} as in (11) and (10). Naturally, the decision should be based on the comparison of J_{CM} and J_{CH} as

$$J_{CM} \underset{CM}{\overset{CH}{\gtrless}} J_{CH}, \tag{13}$$

i.e., the decision rule for each sensor is:

$$\text{A node elects to be } \begin{cases} \text{a nonhead member} & if\, J_{CM} < J_{CH} \\ \text{a cluster head} & if\, J_{CM} > J_{CH} \end{cases} \tag{14}$$

We call this criterion as local energy efficiency criterion, because it is based on only the local information. Substituting (10) and (11) into (13), we obtain

$$\begin{aligned} E_{elec} + \epsilon_{fs} r_{ij}^2 + E_{elec} + E_{DA} + \eta(r_{ij})(E_{elec} + \epsilon_{mp} d_i^4) \\ \underset{CM}{\overset{CH}{\gtrless}} E_{DA} + E_{elec} + \epsilon_{mp} d_j^4. \end{aligned} \tag{15}$$

The benefit range can be obtained by equating two sides though a closed form may be unavailable. Obviously, the cluster radius R_c has to be much smaller than the benefit range because the energy gain is so thin at the outer ring that a new cluster be formed. Although this criterion is too complex to be used in real applications, it promotes using R_c instead of c as the guideline parameter to guide the election. Denote the areas occupied by the whole WSN and the cluster by S_N and S_c respectively,

$$c \approx \frac{S_N}{S_c}. \tag{16}$$

Assume S_N and S_c are both circular, R_c is related to c by

$$c = \frac{\pi R^2}{\pi R_c^2} = (\frac{R}{R_c})^2, \tag{17}$$

where R is the radius of S_N. Although it is mathematically equivalent to partition nodes into c clusters or to organize nodes into clusters with radius R_c, the former is definitely a global approach, which leads to dependence on the global information. Thus, the latter is more suitable for a distributed algorithm.

C. Optimal Cluster Size

As indicated by (17), it is equivalent to determine c or R_c. Here, we try to analytically determine the optimal value of c using the introduced models. This process is similar in some steps to that in [16], which can only determine a rough range , namely $1 < c_{opt} < 6$, for a similar 100-node network, while our analysis predicts the optimal value of R_c in simulation with satisfying accuracy.

The typical scenario is that N nodes are distributed uniformly in a circular region with radius R. There are c clusters with one cluster head and $n-1$ nonhead members within each cluster. n is the average number of cluster members and related to c by

$$n \approx N/c. \tag{18}$$

Based on (12), the average total energy cost can be approximated by

$$\begin{aligned} \bar{J}_{total} &= c(\bar{J}_{CH} + (n-1)\bar{J}_{CM}) \\ &= c\bar{J}_{CH} + (N-c)\bar{J}_{CM} \end{aligned} \tag{19}$$

where $\bar{J}_{CH}$ and $\bar{J}_{CM}$ are the average energy cost for the cluster head and nonhead member respectively.

Following (10) and (11),

$$\bar{J}_{CH} = E_{DA} + E_{elec} + \epsilon_{mp} E[d^4], \tag{20}$$

$$\bar{J}_{CM} = E_{elec} + \epsilon_{fs} E[r^2] + E_{elec} + E_{DA} + E[\eta(r)(E_{elec} + \epsilon_{mp} d^4)]. \tag{21}$$

Since all nodes are placed randomly, r and d are independent, thus, (21) can be written as

$$\bar{J}_{CM} = E_{elec} + \epsilon_{fs} E[r^2] + E_{elec} + E_{DA} + E[\eta(r)](E_{elec} + \epsilon_{mp} E[d^4]). \tag{22}$$

We estimate the expected values in (20) and (22) as follows. Assuming the cluster head is at the center of mass of the cluster,

$$\begin{aligned} E[r^2] &= \int\int_{S_c} r^2 \rho_c(r,\theta) r dr d\theta \\ &= \int_0^{2\pi} \int_0^{R_c} r^2 \rho_c(r,\theta) r dr d\theta \end{aligned} \tag{23}$$

Since the nodes are assumed to be uniformly distributed, $\rho_c(r,\theta)$ is a constant given by

$$\rho_c = 1/\pi R_c^2 = c/(\pi R^2). \tag{24}$$

Substituting (24) and (17) into (23),

$$\begin{aligned} E[r^2] &= \frac{\pi \rho_c R_c^4}{2} \\ &= \frac{R^2}{2c} \end{aligned} \tag{25}$$

Similarly,

$$\begin{aligned} E[\eta(r)] &= \int\int_{S_c}(1-e^{-\alpha r})\rho_c(r,\theta)rdrd\theta \\ &= \frac{c}{\pi R^2}\int_0^{2\pi}\int_0^{R_c}(1-e^{-\alpha r})rdrd\theta \\ &= \frac{2c}{R^2}\int_0^{R_c}(1-e^{-\alpha r})rdr \qquad (26) \\ &= 1+\frac{2c}{\alpha^2R^2}(e^{-\frac{\alpha R}{\sqrt{c}}}(\frac{\alpha R}{\sqrt{c}}+1)-1) \qquad (27) \end{aligned}$$

$$\begin{aligned} E[d^4] &= \int\int_{S_N}|r-r_{BS}|^4\rho_N(r,\theta)rdrd\theta \\ &= \frac{1}{\pi R^2}\int_0^{2\pi}\int_0^{R}(r^2+r_{BS}^2-2rr_{BS}cos(\theta-\theta_{BS}))^2rdrd\theta \qquad (28) \end{aligned}$$

Since $E[d^4]$ is a function of R and irrelevant to c, we keep it in the further derivation.

The optimal value of c can be obtained by setting $\frac{\partial \bar{J}_{total}}{\partial c}$ to zero.

$$\begin{aligned} \frac{\partial \bar{J}_{total}}{\partial c} &= 0 \\ &= \bar{J}_{CH}-\bar{J}_{CM}+(N-c)\frac{\partial \bar{J}_{CM}}{\partial c} \\ &= \epsilon_{mp}E[d^4]-E_{elec}-\epsilon_{fs}\frac{R^2}{2c}-(1+\frac{2c}{\alpha^2R^2}(e^{-\frac{\alpha R}{\sqrt{c}}}(\frac{\alpha R}{\sqrt{c}}+1)-1))(E_{elec}+\epsilon_{mp}E[d^4]) \\ &\quad +(N-c)\frac{\partial E[\eta(r)]}{\partial c}(E_{elec}+\epsilon_{mp}E[d^4])) \qquad (29) \end{aligned}$$

$$\frac{\partial E[\eta(r)]}{\partial c} = \frac{2}{\alpha^2R^2}(e^{-\frac{\alpha R}{\sqrt{c}}}(\frac{\alpha R}{\sqrt{c}}+1)-1)+\frac{e^{-\frac{\alpha R}{\sqrt{c}}}}{c} \qquad (30)$$

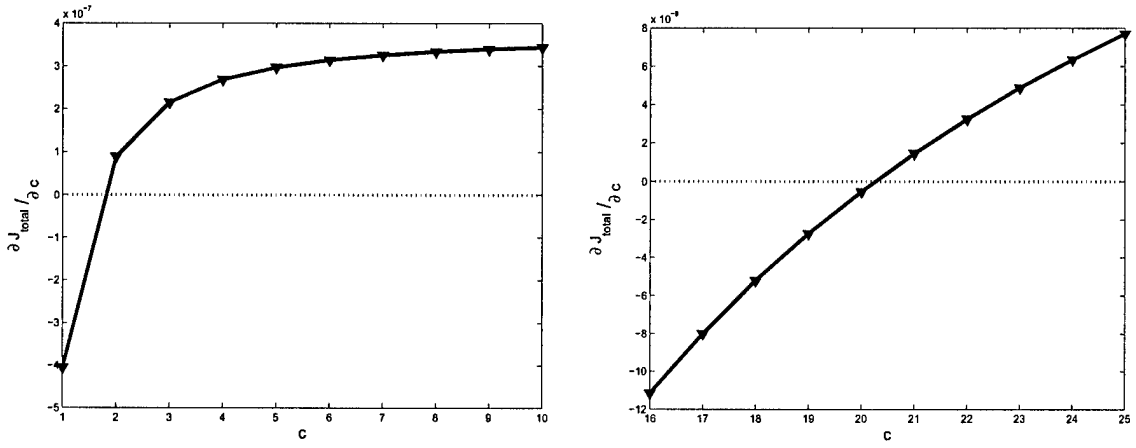
Since it is impossible to solve (29) algebraically, we turn to the numerical solution. For example, the base station is located at $(r_{BS},\theta_{BS})=(125,0)$ and $N=100$, $R=50m$ in our experiments, we can evaluate (28) as

$$E[d^4]=5.8997e+008. \qquad (31)$$

In Fig. 3, we plot $\frac{\partial \bar{J}_{total}}{\partial c}$ over c for $\alpha=0.001$ and $\alpha=0.05$ respectively. The corresponding c_{opt} can be easily obtained as

$$c_{opt} = 1.6569 \quad \text{for } \alpha=0.001, \qquad (32)$$

$$c_{opt} = 20.2600 \quad \text{for } \alpha=0.05. \qquad (33)$$



(a) (b)

Fig. 3. Plot of $\frac{\partial \bar{J}_{total}}{\partial c}$ for $N = 100$, $R = 50m$ and $(r_{BS}, \theta_{BS}) = (125, 0)$.(a)$\alpha = 0.001$. (b)$\alpha = 0.05$.

Observe that $\frac{\partial \bar{J}_{total}}{\partial c}$ is convex at c_{opt}, which indicates $\bar{J}_{total}$ is maximized at c_{opt}. According to (17), the corresponding R_c is

$$R_c = 38m \quad \text{for } \alpha = 0.001, \tag{34}$$

$$R_c = 11m \quad \text{for } \alpha = 0.05. \tag{35}$$

We are also interested in the relation of N to c_{opt}. In Fig. 4, we plot c_{opt} over N for $\alpha = 0.001$ and $\alpha = 0.05$ respectively. These figures show that c_{opt} is a increasing function of N, which indicate the guideline parameter (c or R_c) should be adjusted adaptively if N varies.

V. Expellant Self-Organization

Expellant Self-Organization (ESO) is designed to replace the cluster formation occurring at the beginning of each round in LEACH. As shown in Fig. 5, each node firstly broadcasts its vital information at the maximum radio power level so that the knowledge is spread as widely as possible. The vital information may include nodes' energy, location, etc., though only energy information is needed by ESO. Then, each node counts its neighbors and broadcasts the number of its neighbors locally. "Local broadcast" here means broadcasting at a level corresponding to the cluster radius R_c, which is a predetermined system parameter. If a node's headship potential *qualifies* as a head compared to its neighbors', it will try to claim the headship by broadcasting

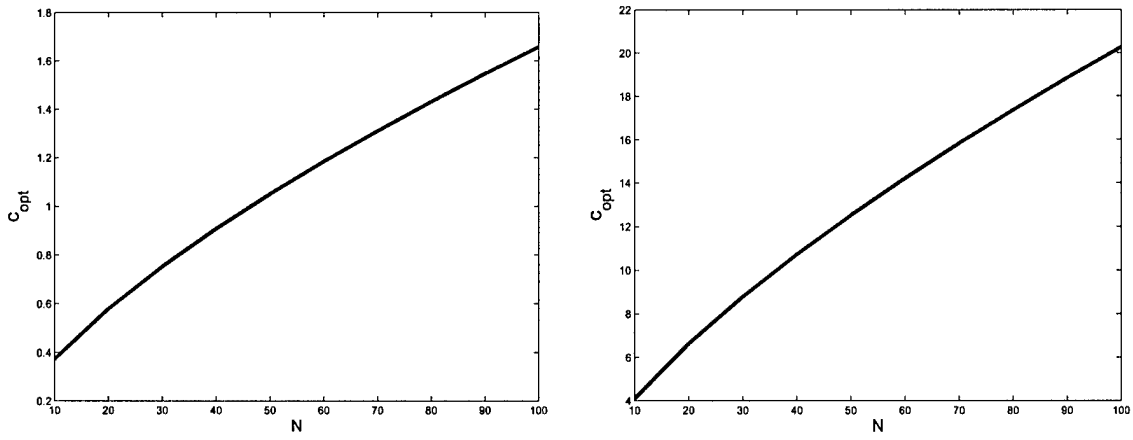


Fig. 4. Plot of c_{opt} vs. $N = 100$ for $R = 50m$ and $(r_{BS}, \theta_{BS}) = (125, 0)$.(a)$\alpha = 0.001$. (b)$\alpha = 0.05$.

locally, which can be viewed as placing a bid for the headship. A node's "neighbors" are defined as the nearby nodes within distance R_c from that node. Due to the possible contention for the headship, such bids could fail, which is indicated by the collision of "headship claims". Using certain back-off strategy, the bidders will contend with each other until a node with satisfactory potential wins. By doing so, the head-to-be expels other possible heads in its neighborhood, and in consequence, the heads are scattered far between.

The headship potential is an important parameter which replaces the self-electing probability used in native LEACH. As discussed in [16], the node's energy is important to determine its potential because the headship can be rotated among nodes by assigning more potential to the nodes with higher energy. In addition, we propose taking the number of neighbors into consideration, because the energy gain is prominent only in the neighborhood of the head as shown in Section IV-B and thus it is energy-efficient to let the node with more neighbors win the headship.

Based on these considerations, the qualification conditions are set as below. For any node, let $\mathcal{N}$ denote the set of its neighbors, $E(i)$ and $B(i)$ be the energy and the number of neighbors of the ith neighbor respectively, $i \in \mathcal{N}$. The thresholds are set as the linear combination of maximum and mean value of corresponding parameters as in (36) and (37) so that the thresholds are adapted

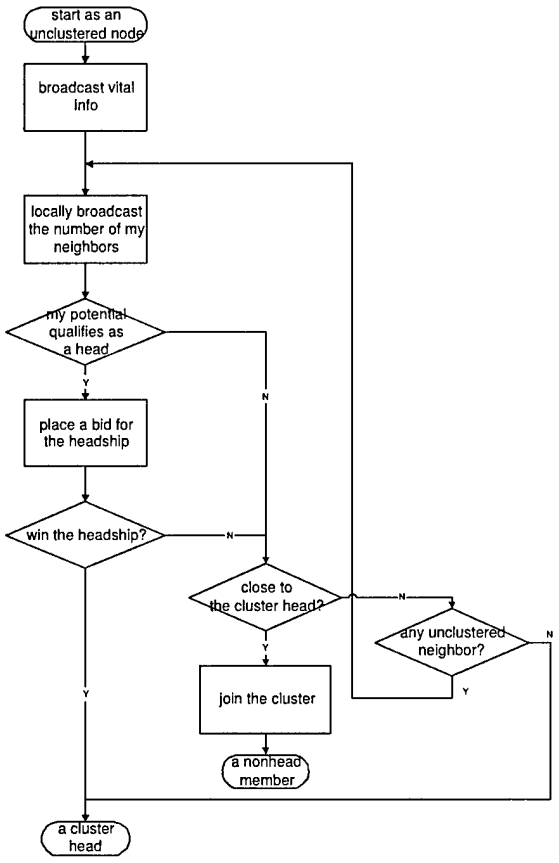


Fig. 5. Flow chart of a node in ESO.

to the current distribution of parameters.

$$E_{Th} = \gamma_1 \max_{i \in \mathcal{N}} E(i) + (1 - \gamma_1) \operatorname{mean}_{i \in \mathcal{N}} E(i) \tag{36}$$

$$B_{Th} = \gamma_2 \max_{i \in \mathcal{N}} B(i) + (1 - \gamma_2) \operatorname{mean}_{i \in \mathcal{N}} B(i) \tag{37}$$

The conditions can be relaxed by decreasing $\gamma_{1,2}$, $\gamma_{1,2} \in [0, 1]$. Since there is no closed-form objective function, it is difficult to determine optimal γ analytically. Fortunately, our experiments show that the performance is not sensitive to the setting of γ. Thus, we simply choose a smaller value for γ_1 and a larger value for γ_2 as $\gamma_1 = 0$, $\gamma_2 = 0.8$, because we want to emphasize the position condition in order to achieve energy efficiency and relax the energy condition in order to allow more nodes into the headship auction.

The nodes qualifying for both conditions are considered as Class A bidders, the nodes qualifying for only one of the conditions are Class B bidders, and the nodes failing both conditions belong to Class C and will not place bids. Class B bidders have delayed starting time compared to Class A so that the former can not bid until waiting long enough to ascertain there are no Class A bidders in their neighborhood. Class B are necessary in order to handle the rare exception that there are no Class A bidders in their vicinity. The extreme case that no heads are elected is avoided by expellant elections by permitting Class B bidders into the headship auction because it is impossible that there are only Class C nodes in the whole network.

Once a node successfully sends out the "headship claim", its neighbors must join it by sending "Request to join". Since these requests can be eavesdropped by their neighbors, their neighbors can correspondingly correct their numbers of unclustered neighbors. If a node finds all its neighbors are clustered, it can elect to be a cluster head by sending out a "headship claim". Those nodes outside the neighborhood of existing cluster heads can not join any clusters. When the public channel is idle again, which indicates there is no node in its neighborhood trying to join existing clusters, another round of auction will begin until all nodes are clustered.

VI. Simulations

In this section, we compare the performance of ESO and LEACH using computer simulations. 100 nodes with 2J initial energy were evenly distributed in a circular region with diameter $100m$, and the base station was located at $(125m, 0)$. Since the set-up overhead is negligible compared with the steady-state traffic, we only count the energy consumption in steady-state phase. We ran 1000 simulations for each case and plotted received data, energy consumption and the number of survival nodes.

A. Optimal c

In this case, the effect of c on energy efficiency was evaluated for nearly perfect data correlation ($\alpha = 0.001$). Fig. 6(a)(b) show the amount of data received at the base station over time and per given amount of data received in the base station. Fig. 6(c)(d) show the number of survival nodes over time and per given amount of energy. Note that there exists a critical phase during which the survival nodes virtually send no data to the base station while they are still alive. The critical phase is indicated by a horizontal line in Fig. 6(a) and a plunging line in Fig. 6(d).

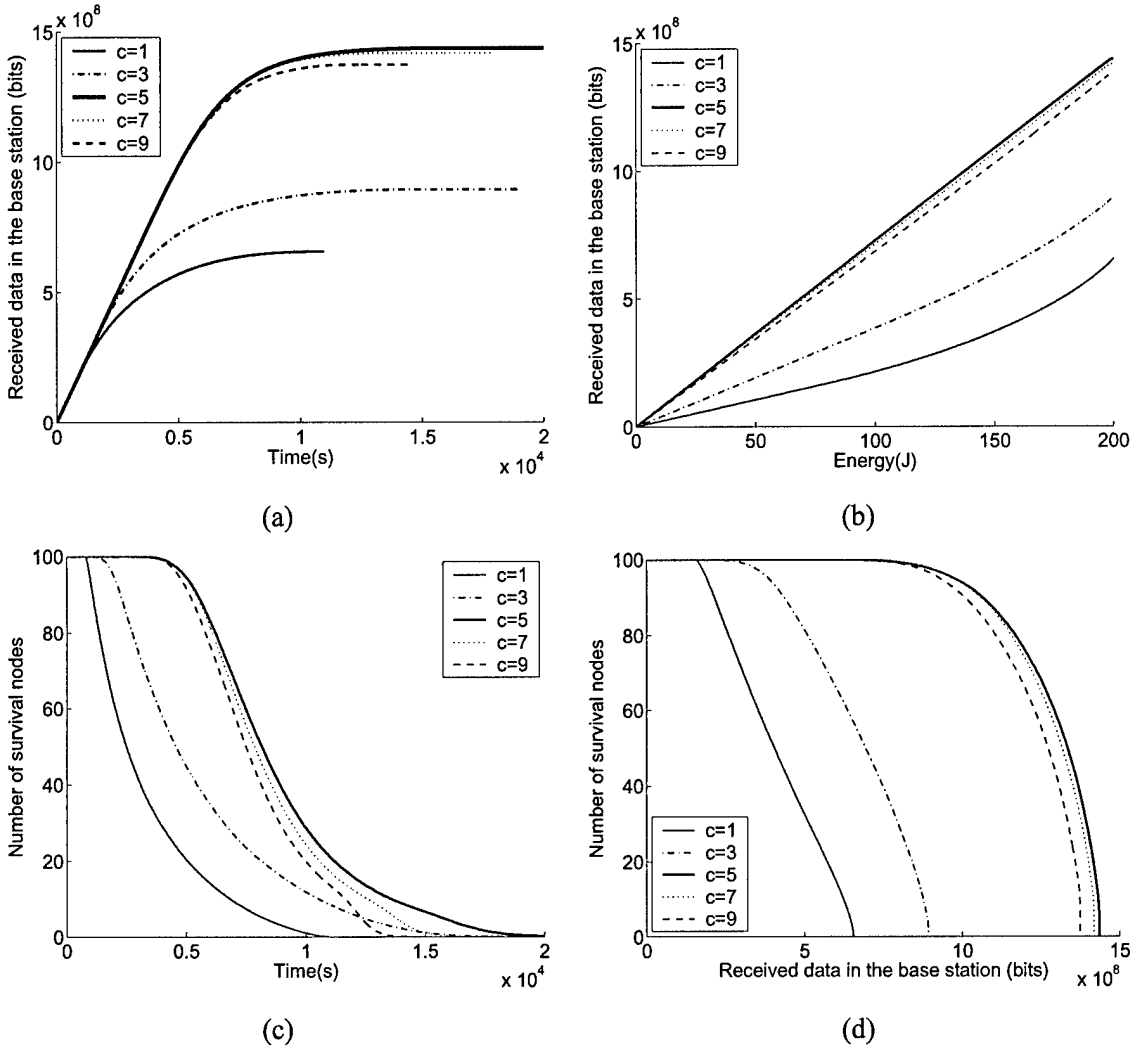


Fig. 6. Data of LEACH at varying c. (a) Amount of data received at the base station over time. (b) Amount of data received at the base station per given amount of energy. (c) Number of survival nodes over time. (d) Number of survival nodes per amount of data received in the base station.

Since some schemes can lengthen the actual lifetime by lengthening the useless critical phase, the actual lifetime is not a fair measurement of energy efficiency. In the following, we choose the effective lifetime whose end is marked by the critical phase.

Taking $c = 3$ and $c = 9$ as examples, although Fig. 6(c) shows the actual lifetime of the former is visibly longer than the latter, Fig. 6(d) distinctly shows the the effective lifetime of

the latter is far longer than that of the former. The reason that $c = 3$ has a longer actual lifetime is that so many nodes dies during the earlier phase that the resulting sparse node distribution favors a lesser c.

Another good measurement of energy efficiency is the ratio of data transportation over energy consumption, termed as Data/Energy Ratio(DER), which is indicated by the slope in Fig. 6(b). Higher slope implies the corresponding scheme can transport more data with given amount of energy consumption. In the following, we use effective lifetime and DER to evaluate the energy efficiency.

Fig. 6(b) and Fig. 6(d) clearly show that both effective lifetime and DER are maximized at $c = 5$. Due to the randomness in the election, the performance does not degrade visibly when c is still close to 5. It is noteworthy that $c = 5$ does not agree with c_{opt} given by the analysis in section IV-C. The main reason is that LEACH can not guarantee that the desired c cluster heads be elected. Suppose no cluster head is elected, i.e.,$c_{elected} = 0$, all nodes have to communicate with the base station directly, in which case all the clustering energy gain is lost. Generally, there is energy penalty when $c_{elected} \neq c$, but the penalty for $c_{elected} = 0$ is disproportionately large because the other cases do not lose the clustering energy gain totally. For $c = 1$, the probability of "$c_{elected} = 0$" is 0.366(shown in Table II), which is intolerably high and reduces the energy efficiency tremendously. While c is set as larger value such as 5, the probability of "$c_{elected} = 0$" decreases to a negligible amount 0.0059 (shown in Table I). The random election and extra energy cost for the case "$c_{elected} = 0$' shift the optimal c to a larger value.

B. ESO vs. LEACH

In this case, Expellant Self-Organization is compared to native LEACH for nearly perfect data correlation ($\alpha = 0.001$). We ran 1000 realizations for each R_c and plotted the effective lifetime and DER. Fig. 7 shows that the performance of ESO is optimal at around $R_c = 40m$ with $DER \approx 7.62E3bits/J$ and effective lifetime around $1.52E9$ s. Compared with those of native LEACH at $c = 5$, ESO shows an approximately 6% improvement for DER and effective lifetime. Denote the time at which the number of survival nodes falls below 10% deadline by $TOD10$ (Time Of Death 10), which indicates the start of the aging period. Fig. 7(b) shows that ESO delays TOD10 by $1.31E9$ bits and thus shorten the aging period. Considering that ESO is a distributed scheme, such improvement demonstrates the energy efficiency of ESO.

TABLE II

OUTCOME OF 100 NODES ELECTING 1 HEAD.

n: number of elected heads	$Pr(n$ elected heads)
0	0.3660
1	0.3697
2	0.1849
3	0.0610
4	0.0149
5	0.0029
6	0.0005
≥ 7	0.0001

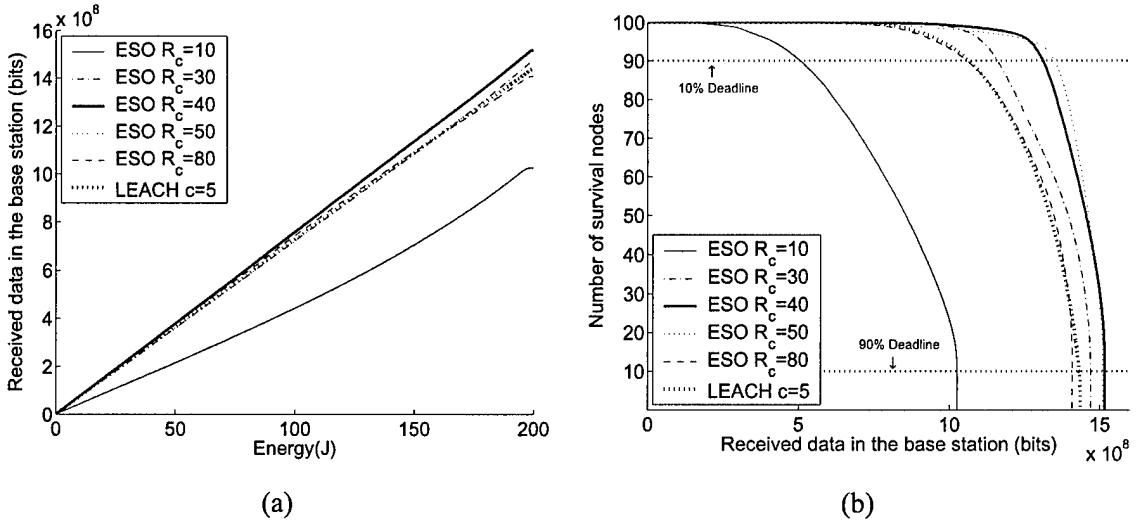


Fig. 7. ESO vs. LEACH. (a) Amount of data received at the base station per given amount of energy. (b) Number of survival nodes per amount of data received in the base station.

The analysis in section IV-C indicates that R_c should be adapted to the decreasing node density. Since the death of nodes decreases the node density, we expect the optimal R_c to decrease accordingly. However, since ESO remarkably delays $TOD10$, the number of survival nodes does not decrease visibly during most of the network lifetime. Therefore, we need not adapt R_c to keep energy efficiency.

C. Data Aggregation Effect On Optimal R_c

In this case, the effect of data aggregation is evaluated. We ran 1000 simulations at different R_c with $\alpha = 0.05$ and plotted the effective lifetime and DER. Fig. 8 shows that the performance

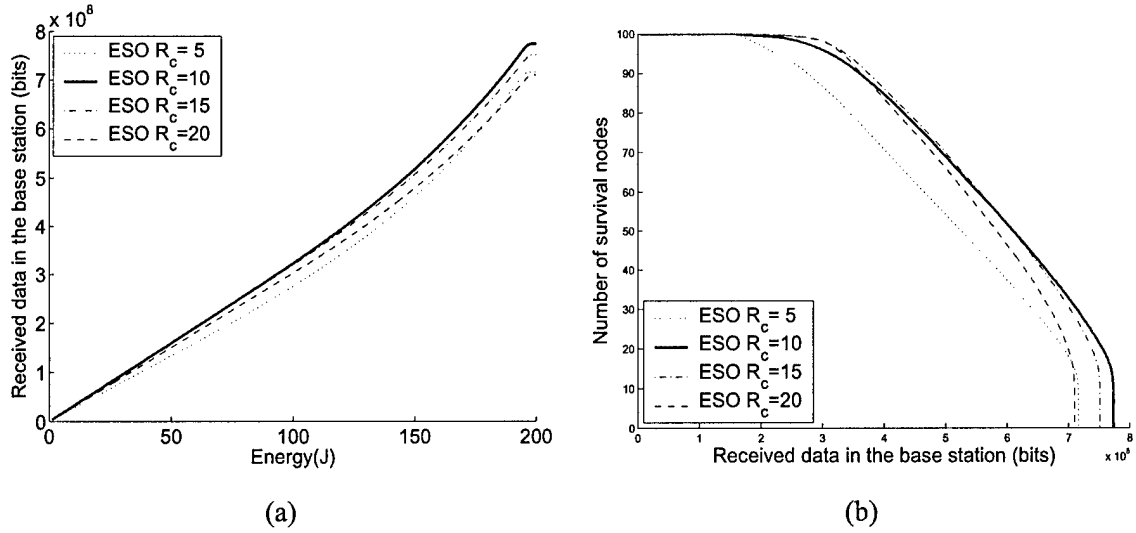


Fig. 8. ESO with $\alpha = 0.05$. (a) Amount of data received at the base station per given amount of energy. (b) Number of survival nodes per amount of data received in the base station.

of ESO is optimal at around $R_c = 10$, which is far from $R_c = 40$ with $\alpha = 0.001$. The reason that the smaller clusters are formed is that the benefit range shrinks when the data correlation decreases. These values of R_c agree with the analysis in section IV-C for both value of α. This shows the advantage of ESO over original LEACH; the election results of ESO conform to the energy-efficient expectation. This also shows the usefulness of our data correlation model; we can easily fit the simulation scenarios for the phenomena of interest by varying α.

VII. Conclusion

The previous clustering researches often take a global approach, which is appropriate for global optimization. However, when a distributed clustering is desired, the already-answered questions such as "How many clusters should the nodes be partitioned into?" have to be translated into a distributed version and restudied. In this paper, we take a fully distributed approach to energy efficiency for WSN. Motivated by the local energy efficiency criterion, we propose

using the cluster size instead of the number of clusters as the guideline parameter in clustering. Furthermore, we utilize the contention for the channel to guarantee the energy-efficient head election. As shown by the simulations, although the proposed ESO uses only local information, it achieves better energy efficiency than native LEACH in terms of Data/Energy Ratio and effective lifetime. The simulations also show that the optimal cluster radius obtained from the experiments agrees well with the analysis of optimal clustering, which indicates the performance of our distributed clustering is close to that of the global optimal one.

VIII. ACKNOWLEDGMENT

This work was supported by the Office of Naval Research (ONR) Young Investigator Award under Grant N00014-03-1-0466.

REFERENCES

[1] I. Akyildiz et al., "A survey on sensor networks," *IEEE Commun. Magazine*,pp.102-114, Aug. 2002

[2] R. Min et al., "Energy-Centric Enabling Technologies For Wireless Sensor Networks," *IEEE Wireless Commun.*, pp 28-39, Aug. 2002

[3] T. Shepard,"A channel access scheme for large dense packet radio networks," in *Proc. ACM SIGCOMM*, Stanford, CA, Aug. 1996, pp.219-230.

[4] M. Ettus, "System capacity, latency and power consumption in multihop-routed SS-CDMA wireless networks," in *Proc. Radio and Wireless Conf. (RAWCON)*, Colorado Springs, CO, Aug. 1998, pp.55-58.

[5] C. R. Lin and M. Gerla, "Adaptive clustering for mobile wireless networks",*IEEE J. Select. Ares Commun.*, vol. 15, pp. 1265-1275, Sept. 1997 D. J. Baker, "Distributed control of broadcast radio networks with changing topologies," in *Proc. IEEE Infocom*, San Diego, CA, Apr. 1983, pp.49-55.

[6] B. Das and V. Bharghavan, "Routing in ad-hoc networks using minimum connected dominating sets," in *Proc. IEEE Int. Conf. Communications*, Montreal, QC, Canada, June 1997, pp. 376-380.

[7] B. Das, R. Sivakumar, and V. Bharghavan, "Routing in ad hoc networks using a spine," in *Proc. IEEE computer Communications and Networks*, pp.34-39,Sept. 1997.

[8] R. Ramanathan and M. Steenstrup, "Hierarchically-organized, multihop mobile wireless networks for quality-of-service support," *Mobile Networks Appl.*, vol. 3, no. 1, pp. 101-119,1998

[9] A. B. McDonald and T. F. Znati, "A mobility-based framework for adaptive clustering in wireless ad hoc networks," *IEEE J. Select. Areas Commun.*, vol. 17, pp. 1466-1487, Aug. 1999

[10] N. H. Vaidya et al., "A cluster-based approach for routing in dynamic networks," *ACM Comput. Commun. Rev.*, vol. 17,no. 2, Apr. 1997.

[11] A. J. Haas and B. Liang, "Ad hoc mobility management with uniform quorum systems," *IEEE/ACM Trans. Networking*, vol. 7, pp. 228-240,Apr. 1999.

[12] W. Chen, N. Jain, and S. Singh, "ANMP:Ad hoc network management protocol," *IEEE J. Select. Areas Commun.*, vol. 17,pp.1506-1531,Aug. 1999

[13] A. Iwata et al., "Scalable routing strategies for ad hoc wireless networks," *IEEE J. Slect. Areas Commun.*, vol. 17,pp.1369-1679,Aug. 1999

[14] T.-C. Hou and T.-J. Tsai, "An Access-Based Clustering Protocol for Multihop Wireless Ad Hoc Networks," *IEEE J. Select. Areas Commun.* , vol. 19, pp. 1201-1210, Jul. 2001

[15] K. Sohrabi et al, "Protocols for Self-Organization of a Wireless Sensor Network," *IEEE Personal Communications*, pp16-27, Oct. 2000

[16] W. B. Heinzelman et al, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," *IEEE Trans. On Wireless Communications*, Vol. 1, No. 4, Oct. 2002

[17] C.F. Chiasserinia and R.R. Rao, "Pulsed battery discharge in communication devices," *Proc. Mobicom*, pp.88-95, 1999

[18] Q. Liang, "A Design Methodology for Wireless Personal Area Networks with Power Efficiency," *IEEE Wireless Communications and Networking 2003*, Vol.3, pp16-20, 2003

[19] T. S. Rappaport, *Wireless Communications:Principles and Practice*, 2nd ed. Upper Saddle River, NJ: Prentice-Hall, 2002.

[20] J.C. Bezdek, *Pattern recognition with fuzzy objective function algorithms*, New York: Plenum Press, 1981.

Energy-Efficient Self-Organization for Wireless Sensor Networks: A Fully Distributed Approach

Liang Zhao[1], Xiang Hong[2], Qilian Liang[3]
Department of Electrical Engineering
University of Texas at Arlington
Arlington, TX 76010, USA
Email: {zhao[1], hong[2]}@wcn.uta.edu, liang[3]@uta.edu

Abstract— **In this paper, we utilize clustering to organize wireless sensors into an energy-efficient hierarchy. We take a fully distributed approach to energy-efficient clustering and propose an Expellant Self-Organization(ESO) scheme that uses expellant election to achieve local energy efficiency. As a distributed scheme using only local information, ESO achieves comparable performance in terms of effective lifetime and Data/Energy Ratio compared with native LEACH that relies on other routing algorithm to access global information. An exponential data correlation model is also introduced to simulate different data aggregation effect.**

I. Introduction

A wireless sensor network(WSN) can be thought of as an *ad hoc* network consisting of sensors linked by a wireless medium to perform distributed sensing tasks. Sensor networks share many communication technologies with *ad hoc* networks, but there are some vital differences such as dense deployment and energy constraint [1], thus the protocols developed for traditional wireless ad hoc networks are not necessarily well suited to the unique features of WSN. When a sensor node may have to operate for a relatively long duration on a tiny battery, energy efficiency becomes a major concern.

A variety of "power-aware" routing protocols have been proposed to address this problem. In one school of thoughts [2]–[4], the traditional Shortest Path First strategy is replaced by Least Energy First routing, i.e., a multihop route is preferred to a single-hop one if only multiple short-distance relays cost less energy than a single long-distance transmission. For example, "Minimum Transmission Energy"(MTE) routing [3], [4] was proposed in place of traditional "minimum hops routing". Another school of thoughts is that nodes are clustered so that a hierarchy is formed. Based on the observations on cellular networks [5]–[13], [19], it would be advisable to partition nodes into clusters for the reasons such as spatial reuse, less update cost, less routing information and less data transmission.

Another dispute in previous *ad hoc* networks research is whether a clusterhead be elected within each cluster. Some researchers [5], [9], [10] argue that it is unreasonable to have a clusterhead as every node has similar energy constraint and the clusterhead will consume energy much faster. Their methodology breaks the information exchange into two parts; cluster members proactively perform the intracluster exchange, and intercluster information exchange is achieved by demand-based operations. This approach does have some advantage when the traffic is mostly within the cluster, however, when the major traffic in WSN is directed from sensor nodes to the base station, i.e., of intercluster type, headless structure suffers from cumbersome intercluster information exchange.

On the other hand, the extra burden of clusterhead can be mitigated by rotating the headship among the members. The rotation can also take advantage of the relaxation effect [17], which indicates frequently reducing the current drawn from the battery enables the battery to recover a portion of its lost capacity and hence lengthens the battery lifetime. In addition, the clusterhead can perform data fusion and reduce the data sent back to the base station. LEACH (Low-Energy Adaptive Clustering Hierarchy) [16], an example of the latter school, can improve network lifetime by an order of magnitude compared with general-purpose multihop approaches. In conclusion, the characteristics of WSN prefer hierarchical structure with clusterheads.

However, the cluster formation in LEACH is based on global information. To access such information, other routing schemes are required. In this sense, LEACH is only a semi-distributed protocol for WSN. The other problem with LEACH is the random head election that can not guarantee that the desired number of cluster heads to be elected or the elected heads are evenly positioned. In this paper, we are concerned to optimize the cluster formation using only local information.

The paper is organized as follows. Section II introduces LEACH and the data correlation model that our research is based on. ESO is described in Section III and simulations are given in Section IV. Section V concludes this paper.

II. Models

A. LEACH

Our energy-efficient clustering research is based on the hierarchy of LEACH which uses a CDMA-TDMA hybrid communication scheme. Each cluster has its own Spread Spectrum code so that the interference between clusters is minimized. For intracluster communications, TDMA slots are assigned for each member to minimize the competition for the shared wireless media. The operation of LEACH is divided into rounds. At the beginning of each round, cluster heads are elected and other nodes join them as members so that N

nodes are partitioned into c clusters. When a cluster is formed, the cluster head creates and broadcasts a time schedule to its members. As shown in Fig.1, each member is assigned a time slot per frame to send its data to its cluster head, and then the cluster head performs data aggregation and sends the resulting data back to the base station. Compared with multihop routing schemes, LEACH shows an outstanding energy efficiency, which can be translated into energy gain.

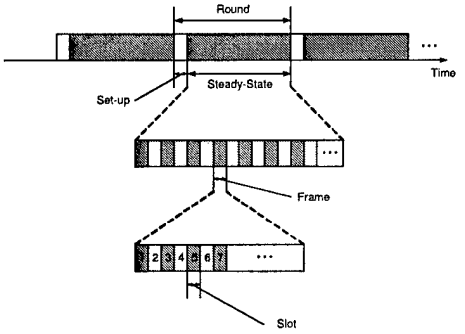


Fig. 1. Time line showing LEACH's frame structure.

However, there are several drawbacks in LEACH's cluster formation as below.

a. **Dependence on global information** In LEACH, each node i elects itself to be a head at the beginning of round $r+1$(which starts at time t) with probability $P_i(t)$. Reference [16] provides two ways to determine the self-electing probability $P_i(t)$. If all nodes are assumed to start with an equal amount of energy, $P_i(t)$ is given by

$$P_i(t) = \begin{cases} \frac{c}{N-c*(r mod \frac{N}{c})} & : C_i(t) = 1 \\ 0 & : C_i(t) = 0 \end{cases}, \quad (1)$$

where c is the desired number of clusters and $C_i(t)$ is the indicator function determining whether or not node i has been a head in the most recent $(r \ mod \ (N/c))$ rounds. The more general estimate of $P_i(t)$ is given by

$$P_i(t) = min\{\frac{E_i(t)}{E_{total}(t)}c, 1\}, \quad (2)$$

where $E_i(t)$ is the current energy(i.e. remaining battery capacity) of node i and

$$E_{total}(t) = \sum_{i=1}^{N} E_i(t). \quad (3)$$

Effectively, N in (1) and E_{total} in (2) are global information, which compromise the distributedness of LEACH.

b. **Random election** Although random decision generally strengthens the robusticity by avoiding sticking to a single choice, too much randomness may shift the decision from the optimal range. In LEACH's case, suppose (1) is used, if N nodes want to elect c heads among them, then the self-electing probability is

$$p = \frac{c}{N} \quad (4)$$

Then the probability of n heads are elected is

$$Pr(n \text{ elected heads}) = \binom{N}{n} p^n (1-p)^{(N-n)} \quad (5)$$

The distribution of the number of elected heads is listed in Table I. In the case of no elected head whose probability listed in row 1, all the nodes have to communicate directly with the base station, in which case all the clustering energy gain is lost. When the number of elected heads is too few, for example, only one head is elected, the head may be exhausted by the tremendous data sent to it. In such cases, the energy efficiency is heavily compromised.

TABLE I
OUTCOME OF 100 NODES ELECTING 5 HEADS.

n: number of elected heads	$Pr(n$ elected heads)
0	0.0059
1	0.0312
2	0.0812
3	0.1396
4	0.1781
5	0.1800
6	0.1500
7	0.1060
8	0.0649
9	0.0349
≥ 10	0.0341

Another problem introduced by the random head selection is that the positions are not taken into consideration. Obviously, the even layout of heads would favor energy efficiency. When heads are randomly selected as in LEACH, elected heads sometimes clump together as shown in Fig.2, which leads to much more energy waste.

B. Data Correlation Model

The data collected by neighboring sensors have a lot of redundancy, thus, [16] assumes perfect data correlation that all individual signals from members of the same cluster can be combined into a single representative signal. Nevertheless, when the cluster size increases to some extent, this assumption can not hold. Therefore, an exponential data correlation model is developed below and used in further discussion.

Considering the phenomenon of interest as a random process, the correlation between data collected by two sensors is generally a decreasing function of the distance r between them. After the data aggregation removes most of the redundancy, the residue can be assumed to be an increasing function of r. Based on the above observation, the data aggregation effect is modeled as below.

Suppose a node collects l bits and sends them back to its head at distance r, the head expends $2lE_{DA}$ Joules to perform data aggregation on the $2l$ bits (collected by itself and its member), where E_{DA} is set as $5nJ/bit$ as in [16]. The resulting data is assumed of $l(1+\eta)$ bits, where η is data aggregation residue ratio and assumed to be complementary exponential, namely,

$$\eta = 1 - e^{-\alpha r}. \quad (6)$$

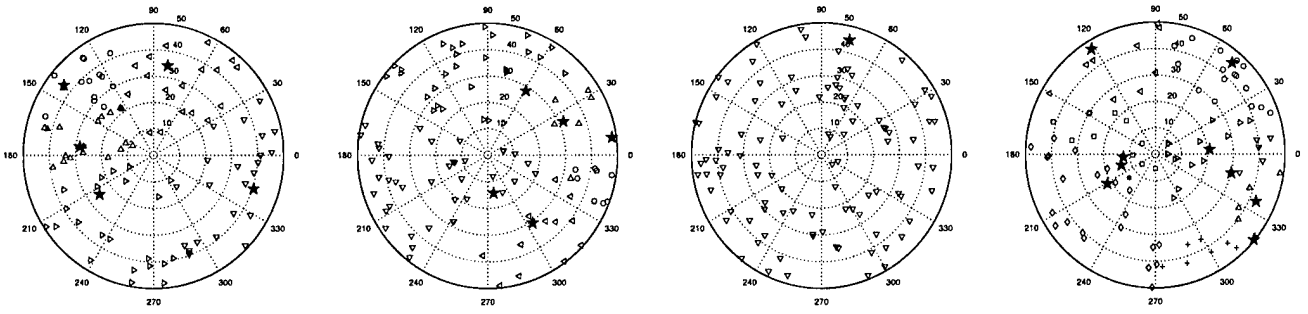


Fig. 2. 100 nodes electing 5 heads(Heads marked by stars). (a) Five heads are elected and evenly distributed. (b) Five heads are elected and clump together. (c) Only one head is elected. (d) Nine heads are elected.

The value of α depends on specific phenomenon of interest. For example, the light, sound and temperature often show a strong correlation at short distance, and thus, α will have smaller values for such data. Since η is a monotonously decreasing function of α and r, η approaches zero for smaller α and r. This model can approach the perfect-data-correlation assumption in [16] by decreasing α or approach the no-data-aggregation assumption in [3], [4] by increasing α, thus, different scenarios can easily be set up by varying α.

C. Radio Energy Dissipation

According to the path loss model [19], the energy required to transmit over a distance d is $E \sim d^{\beta}$, where β is the pass loss exponent, whose value depends on the specific propagation environment. For example, β will have a larger value for long distance transmission than for short distance transmission. To save energy and reduce interference, the power control is widely utilized in wireless communications [19] so that the radio is adjusted for a range of output power level.

The following model is adopted from [16] where perfect power control is assumed. To transmit l bits over distance d, the sender's radio expends

$$E_{TX}(l,d) = \begin{cases} lE_{elec} + l\epsilon_{fs}d^2 & d < d_0 \\ lE_{elec} + l\epsilon_{mp}d^4 & d \geq d_0 \end{cases} \tag{7}$$

and the receiver's radio expends

$$E_{RX}(l,d) = lE_{elec}. \tag{8}$$

And the communication energy parameters are set as d_0=86.2m, E_{elec}=$50nJ/bit$, ϵ_{fs}=$10pJ/bit/m^2$, ϵ_{mp}=$0.0013pJ/bit/m^4$.

III. Expellant Self-Organization

A. Problem Formulation

Clustering has been widely used in pattern recognition, and we use it to obtain the energy-efficient organization for WSN. Using the aforementioned models, the data collected by head k is data-aggregated (with the data collected by its members) and sent back to the base station. Thus, the energy cost for each bit of data collected by head k is

$$J_{CH(k)} = E_{elec} + E_{DA} + \epsilon_{mp}d_k^4, \tag{9}$$

where d_k is the distance between head k and the base station.

Consider nonhead member ki with its head k at the distance r_{ki}, member ki sends its data to head k, and then head k performs data aggregation on the data and sends the resulting data to the base station. Thus, the energy cost for each bit of data collected by member ki is

$$J_{CM(ki)} = E_{elec}+\epsilon_{fs}r_{ki}^2+E_{elec}+E_{DA}+\eta(r_{ki})(E_{elec}+\epsilon_{mp}d_k^4). \tag{10}$$

Considering all c clusters, the overall cost is

$$J_{total} = \sum_{i=1}^{c}\{J_{CH(k)} + \sum_{i\in\Lambda_k} J_{CM(ki)}\}, \tag{11}$$

where Λ_i is the set of members of cluster k.

Taking $E[J_{total}]$ the expected value of the overall energy cost as the objective function, the original problem is translated into an objective function clustering [20]. If a central control scheme is possible, an iterative algorithm can be run at the base station to minimized $E[J_{total}]$. For example, Fuzzy c-Means is utilized in [18] to minimize an Euclidean-distance-based functional representing the energy cost in Wireless Personal Area Networks. However, since WSNs are working in *ad hoc* mode, clustering decision must be distributed to each sensor node. Thus, our goal is using only local information to achieve energy-efficient clustering.

Generally, if a node is close to a cluster head, there is some energy gain if it joins that cluster. The energy gain diminishes when the distance between the nonhead member and the head increases. Consequently, the energy gain approaches zero at some critical distance, termed as benefit range. To determine the benefit range, consider a node with a head at distance r. The node could choose to be a nonhead member or a head, which would consequently cost J_{CM} or J_{CH} as in (10) and (9). Naturally, the decision should be based on the comparison of J_{CM} and J_{CH} as

$$J_{CM} \gtrless J_{CH} \tag{12}$$

Applying this criterion to the data correlation model and the energy dissipation model presented in Section II, i.e., substituting (10) and (9) into (12), we obtain

$$E_{elec} + \epsilon_{fs} r_{ki}^2 + E_{elec} + E_{DA} + \eta(r_{ki})(E_{elec} + \epsilon_{mp} d_k^4) \gtrless E_{elec} + E_{DA} + \epsilon_{mp} d_i^4. \quad (13)$$

The benefit range can be obtained by equating two sides though an explicit form may not be available. Obviously, the cluster radius R_c has to be much smaller than the benefit range because the energy gain is so thin at the outer ring that a new cluster be formed. Based on this observation, we use R_c instead of c as the system parameter to guide the election. Assuming the the zones occupied by the whole WSN and the cluster are both circular, R_c is related to c by

$$c \approx \frac{\text{network area}}{\text{cluster area}} = \frac{\pi R^2}{\pi R_c^2} = (\frac{R}{R_c})^2, \quad (14)$$

where R is the radius of the zone occupied by the WSN. Although it is mathematically equivalent to partition nodes into c clusters or to organize nodes into clusters with radius R_c, the former is definitely a global approach, which leads to dependence on the global information. Thus, the latter is more suitable for a distributed algorithm.

B. ESO Description

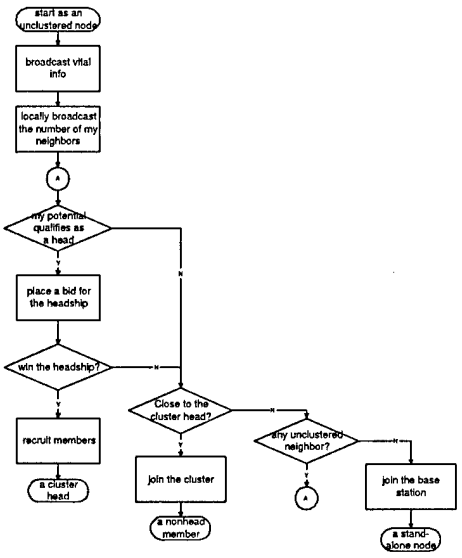


Fig. 3. Flow chart of a node in ESO.

Expellant Self-Organization(ESO) is designed to replace the cluster formation occurring at the beginning of each round in LEACH. As shown in Fig.3, first, each node broadcasts its vital information at the maximum radio power level so that the knowledge is spread as wide as possible. The vital information may include nodes' energy, location, etc., but only energy information is needed by ESO. Then, each node counts its neighbors and broadcasts the number of its neighbors locally. "Local broadcast" here means broadcasting at the level corresponding to the cluster radius R_c, which is a predetermined system parameter. If a node's headship potential *qualifies* as a head compared to its neighbors', it will try to claim the headship by broadcasting locally, i.e., place a bid for the headship. "Neighbors" means the nearby nodes which are within distance R_c. Due to the possible contention for the headship, such bids could fail, which is indicated by the collision of "headship claims". Using certain back-off strategy, the bidders will contend with each other until a node with satisfactory potential wins. By doing so, the head-to-be expels other possible heads in its neighborhood, and in consequence, the heads are scattered far between.

The headship potential is an important parameter which replaces the self-electing probability in native LEACH. As discussed in [16], the node's energy is important to determine its potential because the headship can be rotated among nodes by assigning more potential to the nodes with higher energy. In addition, we propose taking the number of neighbors into consideration, because the energy gain is prominent only in the neighborhood of the head as shown in Section III-A and thus it is energy-efficient to let the node with many neighbors win the headship.

The qualification conditions are set as below. For any node, let $\mathcal{N}$ denote the set of its neighbors, $E(i)$ and $B(i)$ be the energy and the number of neighbors of the i^{th} neighbor respectively. The thresholds are set as the linear combination of maximum and mean value of corresponding parameters as in (15) and (16) so that the thresholds vary adaptively according to the current distribution of parameters.

$$E_{Th} = \gamma_1 \max_{i \in \mathcal{N}} E(i) + (1 - \gamma_1) \operatorname{mean}_{i \in \mathcal{N}} E(i) \quad (15)$$

$$B_{Th} = \gamma_2 \max_{i \in \mathcal{N}} B(i) + (1 - \gamma_2) \operatorname{mean}_{i \in \mathcal{N}} B(i) \quad (16)$$

The conditions can be relaxed by decreasing $\gamma_{1,2}$, $\gamma_{1,2} \in [0, 1]$. Since there is no closed-form objective function, it is difficult to determine γ analytically. In our experiments, the performance is not sensitive to the setting of γ. Thus, we choose a smaller value for γ_1 and a larger value for γ_2 as $\gamma_1 = 0$, $\gamma_2 = 0.8$, because we emphasize the position condition in order to achieve energy efficiency and relax the energy condition in order to accept more nodes as bidders.

The nodes qualifying for both conditions are considered as Class A bidders, the nodes qualifying for only one of the conditions are Class B bidders, and the nodes failing both conditions will not place a bid. Class B bidders have delayed starting time compared to Class A so that the former will not bid until waiting long enough to ascertain there are no Class A bidders in their neighborhood. Class B is set up to handle the rare exception that there is no Class A bidders in their vicinity. The extreme cases that no or too few heads are elected are avoided by expellant elections.

Once a node successfully sends out the "headship claim", its neighbors will join it by sending "Request to join". Since these requests can be eavesdropped by their neighbors, their neighbors can correct their numbers of unclustered neighbors corresponding. If a node finds all its neighbors are clustered,

it sends a "Request-to-join" to the base station and becomes a "stand-alone" node who communicates directly with the base station. The existence of stand-alone nodes is due to the fact that some nodes are so close to the base station that there is no clustering energy gain for them. Those nodes who are outside the neighborhood of existing cluster heads will not try to join any clusters. When such a node finds that the public channel is idle again (which means there is no node in its neighborhood trying to join existing clusters), it can place a bid for the headship if it still qualifies as a cluster head. Then another round of bid will begin until all nodes are clustered (including those stand-alone nodes who choose the base station as their cluster head).

IV. Simulations

In this section, we compare the performance of ESO and LEACH using computer simulations. 100 nodes with 2J initial energy were evenly distributed in a circular region with diameter of 100 m, and the base station was located at $(125m, \pi/2)$. We ran 1000 simulations for each case and plotted received data, energy dissipation and the number of survival nodes.

A. Optimal c

In this case, the effect of c on energy efficiency was evaluated for perfect data correlation (α in (6) is set as 0.001). Fig.4(a)(b) shows the amount of data received at the base station over time and per given amount of energy. Fig.4(c)(d) shows the number of survival nodes over time and per given amount of energy. It is noted that there exists a critical phase during which the survival nodes virtually send no data to the base station while they are still alive. The critical phase is indicated by a vertical line in Fig.4(a) and a plunging line in Fig.4(d). The reason for the critical phase is that these nodes still try in vain to organize themselves into clusters but have no successful transmission. Since some schemes can lengthen the actual lifetime by lengthening the useless critical phase, the actual lifetime is not a fair measurement of energy efficiency. In the following, we choose the effective lifetime whose end is marked by the critical phase.

Taking $c = 3$ and $c = 9$ as examples, although Fig.4(c) shows the actual lifetime of the former is visibly longer than the latter, Fig.4(d) distinctly shows the the effective lifetime of the latter is far longer than that of the former. The reason that $c = 3$ has a longer actual lifetime is that so many nodes dies during the earlier phase that the resulting sparse node distribution favors a lesser c.

Another good measurement is the data transportation over energy dissipation, termed as Data/Energy Ratio(DER), which is indicated by the slope in Fig.4(b). Higher slope implies the corresponding scheme can transport more data with given amount of energy dissipation. In the following, we use effec-

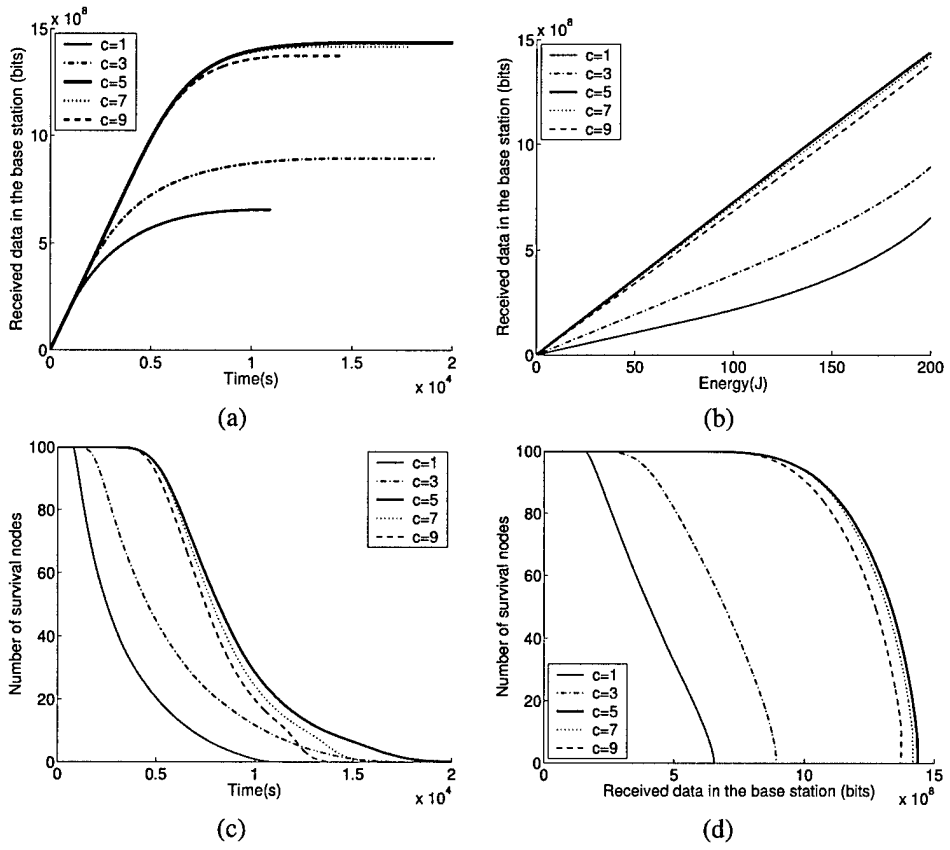


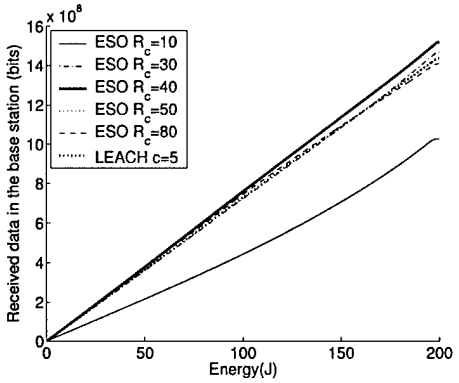
Fig. 4. Data of LEACH at varying c. (a) Amount of data received at the base station over time. (b) Amount of data received at the base station per given amount of energy. (c) Number of survival nodes over time. (d) Number of survival nodes per given amount of energy.

tive lifetime and DER to evaluate the energy efficiency.

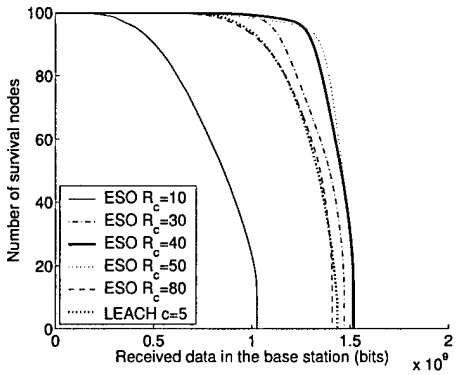
Fig.4(b) and Fig.4(d) clearly show that both effective lifetime and DER are maximized at $c = 5$. Due to the randomness in the election, the performance does not degrade visibly when c is still close to 5.

B. ESO vs. LEACH

In this case, Expellant Self-Organization is compared to native LEACH for perfect data correlation (α in (6) is set as 0.001). We ran 1000 simulations for each R_c and plotted the effective lifetime and DER. Fig.5 shows the performance



(a)



(b)

Fig. 5. ESO vs. LEACH. (a) Amount of data received at the base station per given amount of energy. (b) Number of survival nodes per given amount of energy.

of ESO is optimal at around $R_c = 40m$ with $DER \approx 7.62E3bits/J$ and effective lifetime around $1.52E9\ s$. Compared with those of native LEACH at $c = 5$, ESO shows an approximately 6% improvement for DER and effective lifetime. Considering that ESO is a distributed scheme, such improvement demonstrates the energy efficiency of ESO.

Substituting $R_c \approx 40m$ into (14), we obtain $c \approx 1.56$, which is less than $c_{opt} \approx 5$ obtained in Section IV-A. There are two reasons for this difference.

a. As shown in Section IV-A, when c varies near 5, the performance does not degrade visibly. However, when c is set near zero, the probability of "no head are elected" surges up as shown in Table II. For this case, the energy cost is much larger than other cases because there is totally no clustering energy gain. The random election and extra energy cost for the case "no head are elected" shift the optimal c to a larger value.

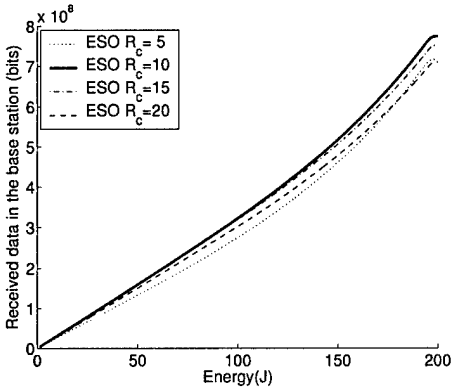
TABLE II
OUTCOME OF 100 NODES ELECTING 1 HEAD.

n: number of elected heads	$Pr(n$ elected heads$)$
0	0.3660
1	0.3697
2	0.1849
3	0.0610
4	0.0149
5	0.0029
6	0.0005
≥ 7	0.0001

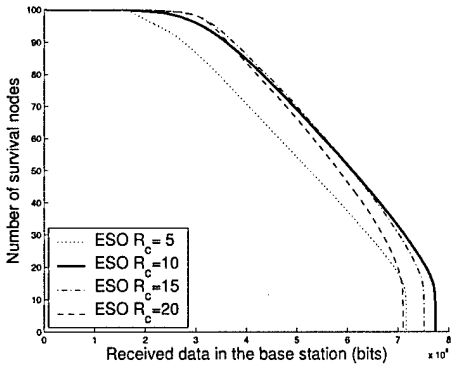
b. ESO permits nodes to communicate directly with the base station if they can not find appropriate clusters to join. These stand-alone nodes are not counted as clusters, which leads to less clusters for ESO.

C. Data Aggregation Effect On Optimal R_c

In this case, the effect of data aggregation is evaluated. We ran 1000 simulations at different R_c with α fixed at 0.05 and compare the effective lifetime and DER with those with $\alpha = 0.001$. Fig.6 shows that the performance of ESO is optimal at



(a)



(b)

Fig. 6. ESO with $\alpha = 0.05, 0.001$. (a) Amount of data received at the base station per given amount of energy. (b) Number of survival nodes per given amount of energy.

around $R_c = 10$, which is far from $R_c = 40$ with $\alpha = 0.001$.

The reason that the smaller clusters are formed is that the benefit range shrinks when the data correlation decreases. This shows the usefulness of our data correlation model; we can easily fit the simulation scenarios for the phenomena of interest by varying α.

V. Conclusion

The previous clustering researches often take a global approach, which is appropriate for global optimization. However, when a distributed clustering is desired, the already-answered questions such as "How many clusters should the nodes be partitioned into?" have to be translated into a distributed version and restudied. We take a distributed approach to energy efficiency for WSN and propose Expellant Self-Organization that uses expellant election to achieve local energy efficiency. Although ESO uses only local information, it achieves comparable energy efficiency with native LEACH in terms of effective lifetime and Data/Energy Ratio.

VI. Acknowledgment

This work was supported by the Office of Naval Research(ONR) Young Investigator Award under Grant N00014-03-1-0466.

References

[1] I. Akyildiz et al., "A survey on sensor networks," *IEEE Commun. Magazine*,pp.102-114, Aug. 2002

[2] R. Min et al., "Energy-Centric Enabling Technologies For Wireless Sensor Networks," *IEEE Wireless Commun.*, pp 28-39, Aug. 2002

[3] T. Shepard,"A channel access scheme for large dense packet radio networks," in *Proc. ACM SIGCOMM*, Stanford, CA, Aug. 1996, pp.219-230.

[4] M. Ettus, "System capacity, latency and power consumption in multihop-routed SS-CDMA wireless networks," in *Proc. Radio and Wireless Conf. (RAWCON)*, Colorado Springs, CO, Aug. 1998, pp.55-58.

[5] C. R. Lin and M. Gerla, "Adaptive clustering for mobile wireless networks",*IEEE J. Select. Ares Commun.*, vol. 15, pp. 1265-1275, Sept. 1997 D. J. Baker, "Distributed control of broadcast radio networks with changing topologies," in *Proc. IEEE Infocom*, San Diego, CA, Apr. 1983, pp.49-55.

[6] B. Das and V. Bharghavan, "Routing in ad-hoc networks using minimum connected dominating sets," in *Proc. IEEE Int. Conf. Communications*, Montreal, QC, Canada, June 1997, pp. 376-380.

[7] B. Das, R. Sivakumar, and V. Bharghavan, "Routing in ad hoc networks using a spine," in *Proc. IEEE computer Communications and Networks*, pp.34-39,Sept. 1997.

[8] R. Ramanathan and M. Steenstrup, "Hierarchically-organized, multihop mobile wireless networks for quality-of-service support," *Mobile Networks Appl.*, vol. 3, no. 1, pp. 101-119,1998

[9] A. B. McDonald and T. F. Znati, "A mobility-based framework for adaptive clustering in wireless ad hoc networks," *IEEE J. Select. Areas Commun.*, vol. 17, pp. 1466-1487, Aug. 1999

[10] N. H. Vaidya et al., "A cluster-based approach for routing in dynamic networks," *ACM Comput. Commun. Rev.*, vol. 17,no. 2, Apr. 1997.

[11] A. J. Haas and B. Liang, "Ad hoc mobility management with uniform quorum systems," *IEEE/ACM Trans. Networking*, vol. 7, pp. 228-240,Apr. 1999.

[12] W. Chen, N. Jain, and S. Singh, "ANMP:Ad hoc network management protocol," *IEEE J. Select. Areas Commun.*, vol. 17,pp.1506-1531,Aug. 1999

[13] A. Iwata et al., "Scalable routing strategies for ad hoc wireless networks," *IEEE J. Slect. Areas Commun.*, vol. 17,pp.1369-1679,Aug. 1999

[14] T.-C. Hou and T.-J. Tsai, "An Access-Based Clustering Protocol for Multihop Wireless Ad Hoc Networks," *IEEE J. Select. Areas Commun.* , vol. 19, pp. 1201-1210, Jul. 2001

[15] K. Sohrabi et al, "Protocols for Self-Organization of a Wireless Sensor Network," *IEEE Personal Communications*, pp16-27, Oct. 2000

[16] W. B. Heinzelman et al, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," *IEEE Trans. On Wireless Communications*, Vol. 1, No. 4, Oct. 2002

[17] C.F. Chiasserinia and R.R. Rao, "Pulsed battery discharge in communication devices," *Proc. Mobicom*, pp.88-95, 1999

[18] Q. Liang, "A Design Methodology for Wireless Personal Area Networks with Power Efficiency," *IEEE Wireless Communications and Networking 2003*, Vol.3, pp16-20, 2003

[19] T. S. Rappaport, *Wireless Communications:Principles and Practice*, 2nd ed. Upper Saddle River, NJ: Prentice-Hall, 2002.

[20] J.C. Bezdek, *Pattern recognition with fuzzy objective function algorithms*, New York: Plenum Press, 1981.

Latency-aware and Energy Efficiency Tradeoffs for Wireless Sensor Networks

Xinsheng Xia
Department of Electrical Engineering
The University of Texas at Arlington
416 Yates Street
Nedderman Hall, Rm 541
Arlington, TX 76010
Email: xia@wcn.uta.edu

Qilian Liang
Department of Electrical Engineering
The University of Texas at Arlington
416 Yates Street
Nedderman Hall, Rm 541
Arlington, TX 76010
Email: liang@uta.edu

Abstract— **Performance evaluation is one of the most important research topics for the Wireless Sensor Networks (WSN). Latency-aware and energy efficiency are two important parameters to evaluate the networks quality. In order to meet different performance requirements of the service, we classify the packets into high priority and low priority. We consider the latency and energy tradeoffs in WSN. The latency of the high priority packets is small but the network cost more energy. The latency of the packets of low priority packets is large but the network cost less energy. We solve this problem by transmitting redundant packets in the WSN. We assume that the network has a cell-partitioned structure, and sensor moves according to one-step Markov path model with constant speed. Simulation shows that the scheduling algorithm with/without redundancy can realize the latency/energy tradeoffs in WSN.**

I. Introduction

Wireless sensor networks are likely to be widely deployed in commercial and military applications. However, several obstacles need to be overcome, such as latency-aware and energy efficiency [1] [2]. Latency-aware means to transfer the packets among sensors as quickly as possible. Energy efficiency means to the networks should function for as long as possible.

The cell-partitioned model is adopted in this paper (see Figure 1). We can assume that the network is divided into non-overlapping cells, each cell is of equal size [3]. So we can get:

- N=Number of sensor nodes
- C=Number of cells
- D=N/C=User/Cell Density

The sensors are roaming independently from cell to cell. If two sensors are in the same cell, they can transfer packets with each other, and sensors within different cells cannot communicate with each other. The sensors have a constant mobility speed and actual mobility can be described by one-step Markov path model [4]. Each sensor can generate packets with a Poisson distribution and each sensor can reserve originally generated packets and relay packets. There are C subqueues in one sensor and each packet enters its subqueue according to its destination address. This model can simplify the scheduling complexity and facilitates analysis. It can also conceal the detail of global network topology from individual sensor node [5].

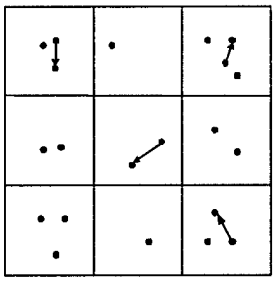


Fig. 1. A cell-partitioning wireless sensor network

In this paper, we consider the tradeoffs between the delay performance and the energy efficiency offered by the cell partitioned wireless model. The contributions are twofold: First, we classified the sensor service into two priorities: high and low. The higher priority, the better delay performance and more energy consumption. We realized it with the two-hop relay algorithm. Second, we establish energy/delay tradeoffs curve for the performance of the two-hop relay algorithm.

In order to evaluate the algorithm, we need to understand the major parameters about the wireless sensor network.

A. Latency

Because data communications in the sensor networks has trimming constraints, it is important to design the network algorithm to meet a kind of end-end deadlines [6]. Packet in the networks is required to meet different end-end deadline, so we need to assign a priority to each packet.

B. System lifetime

It is not convenient to recharge the sensor node battery, so the energy efficiency is extremely important for sensor network. The network should keep a enough number of "live" sensor nodes to collect enough information, which means the network need to keep the energy among the sensor nodes in balance. So the remaining battery capacity and the remaining

alive sensor nodes are two parameters of the network system lifetime.

C. Network efficiency

The function of the sensor network is to collect data and transfer packets and the amount of packets transmitted is one of the parameters to evaluate the networks efficiency. The energy consumed when the sensor transmits and receives the packets will be much more than that consumed when the sensor node is idle.

The rest of this paper is organized as follows. In section II, we introduce the energy, delay and the 2-hop relay algorithm. In section III, we introduce the scheduling algorithm. In section IV, we introduce the simualtion result. In section V, we conclude this paper.

II. Energy,Delay And The 2-Hop Relay Algorithm

A. Energy

A sensor node consumes significant power when it either transmits a packet or when it receives a packet. It will also consume energy when the sensor node is idle because the sensor node keeps moving. The energy consumption ratio of Transmit: Receive: Idle is approximately 40:20:1 [7].

B. Delay

The packet transmission latency between the sensors includes three parts: the wireless channel transmission delay, the Physical/MAC layer delay, and the queuing delay.

Defined D as the distance between two sensors and C as the light speed, the wireless channel transmission delay as:

$$Delay_{ch} = \frac{D}{C} \tag{1}$$

The Physical/MAC layer delay will be decided by interaction of the transmitter and the receive channel, the sensor density and the sensor traffic intensity etc.

The queuing delay is decided by the sensor I/O system processing rate, the subqueue length in the sensor and especially the probability that a source-destination pair exits within the cell. The degree of mobility is a key parameter. In this mobility model, the higher speed, the lower transmission delay.

In order to make the system "stable", the rate at which sensor node transfers packets intended for its destination must satisfy all sensors that the queuing lengths will not be infinite and the average delays will be bounded.

C. The Two-hop Relay Algorithm

This relay algorithm restricts packets to 2-hop paths, and the relay packet is inserted into the subqueue of the relay sensors until a source encounters its destination.

We summarize the two-hop relay algorithm as follows [8]:

1)If there exists source-destination pairs within the cell, there are two options:

- If there exists one source-destination pair within the cell and if the source contains a new packet intended for that destination, transmit.
- If there exists more than one source-destination pair within the cell, choose the sensor with the longest subsequeue as the source and choose the sensor with the energy most as the destination and transmit it.

2)If there is no source-destination pair in the cell, there are two options:

- Send a Relay packet to its destination: if the designated transmitter has a packet destined for the designated receiver, send the packets to the receiver.
- Send a new relay packet:
  1) For high priority sensor: if the designated transmitter has a new packet that has never before been transmitted, conserve the packet in its own subqueue according to its destination. Choose the three energy most sensors as the relay destinations and transmit three copies to them.
  2) For low priority sensor: conserve the packet in its own subqueue according to its destination.

This algorithm restricts all routes to 2-hop while the relay packets are only allowed to transmit to their destinations. We pick up the packet reserved in the subqueue with the longest queuing length to keep the queuing length in balance among the sensors in order to reduce the time jitter. We choose the sensors with most energy as the destination to keep the energy in balance among sensors.

III. Scheduling algorithm

The effect of transmitting redundant packets will consume more energy, however, it will also increase the chance that the sensor nodes which hold the original or relay packets to reach their destination. According to the latency performance parameter, we assigned the packets with high and low priorities.

When the networks transmit the high priority packet, it will schedule with redundancy. Because redundancy can improve delay, the high priority packets can get better delay performance than that of low priority. Transmitting and receiving redundant packets will cause more energy consumption; but of cause the scheduling algorithm with redundancy will shorten the lifetime of the wireless sensor networks.

In the previous section, the two-hop relay algorithm is introduced and it is used to send a single packet to a single destination. When we use algorithm in the wireless sensor networks, more complications arise. We propose more scheduling algorithms to overcome these complications.

A. Cell location algorithm

Each sensor node knows its location (X position, Y position). As all the cells are of the same size, each sensor node can determine the cell serial number it belongs to.

For example, the network size is $N \times N$ and it is partitioned into $C = S^2$ cells:

$$Cell_{sn} = [\frac{X \cdot S}{N}] + [\frac{Y \cdot S}{N}] \cdot S + 1 \tag{2}$$

Where [ ] refers to the round function, the round function will round the value of the float argument to the nearest integer value.

Every sensor will send a "Hello" message with its cell serial number $Cell_{sn}$ and other information to other sensor between a constant time interval. When a sensor with ID number A receives a "Hello" message sent by sensor B, sensor A compares its cell serial number $Cell_{sna}$ with the cell serial number $Cell_{snb}$ of sensor B.

- If $Cell_{sna}$ is equal to $Cell_{snb}$, that means sensor A and sensor B are in the same cell and the information of sensor already in the database of sensor B, update the information of sensor B.
- If $Cell_{sna}$ is equal to $Cell_{snb}$, that means sensor A and sensor B are in the same cell but the information of sensor is not in the database of sensor B, record the information of sensor B.
- If $Cell_{sna}$ not equal to $Cell_{snb}$, that means sensor A and sensor B are not in the same cell but the information of sensor is in the database of sensor B, delete the information of sensor B.
- If $Cell_{sna}$ not euqal to $Cell_{snb}$, that means sensor A and sensor B are in the same cell but the information of sensor is not in the database of sensor B, remain idle.

Notice that a sensor only keeps the information of the sensors that in the same cell and keeps updating it. The sensor can reduce the memory usage and keep the latest information.

B. In-cell feedback algorithm

As there is redundancy in the network, when a packet has been delivered to its destination, its remnant versions of this packet should be removed from the network. We assume all the packets have a send serials number(SN). SN combining with source sensor ID is unique in the network. When a sensor node A receives a packet, it will send out a "notice" message with its SN $Packet_{sn}$, source sensor ID B and destination sensor ID A.

When a sensor receives the "notice" message, it will search packet with SN in the A subqueue. If there is a packet with SN $Packet_{sn}$, source sensor ID B and destination sensor ID A, remove it from the subqueue. Otherwise, remain idle.

Notice that, no packet will transmit to its destination twice. So we can reduce the energy consumption and shorten average delay.

IV. Simulation

We implemented the simulation model using the OPNET modeler. The simulation region is 180×180 meters, and it is divided into 9 non-overlapping cells. Each cell is of equal size, that is 60×60 meters. In the previous section, we know that the energy consumption ratio is 40:20:1. So we can assume that the sensor node consumes approximately 3×10^{-5} watts when idle, 1.2×10^{-3} watts during transmissions and 6×10^{-4} watts during reception.

There are 40 sensor nodes in the simulation model, and the sensors are roaming independently with the ground speed 4 m/s. The mobility model is called one-step Markov path model. The probability of moving in the same direction as the previous move is higher than other directions in this model; That means this model has memory. Fig.2 shows the probability of the six directions.

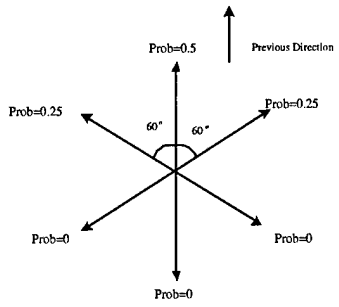


Fig. 2. One-step Markov path model

1) Average Latency: We use the average latency parameter (see equation 3.) to evaluate the network performance. It is the average transmission delay of the entire received packet, which is in the same priority. Each packet is labeled a timestamp when it was generated by the source sensor node. When its destination sensor node receives it, the time interval is the transmission delay.

$$Average\ Latency = \frac{\sum_{i=1}^{K} D_i}{K} \tag{3}$$

Observe Fig.3 the latency performance of the algorithm with redundancy for high priority packets is much better than that of the algorithm without redundancy for the low priory packets. Not only the average delay of high priority packets is much smaller than that of the low priority packets, but also the time jitter is much better. Time jitter refers to short-term variation or instability in the duration of a specified time interval. We can draw a conclusion: if the service is time-sensitive, such as video or audio service, we can adopt the scheduling algorithm with redundancy to improve their delay performance.

2) Energy Efficiency: The algorithm for high priority packets uses the multicast technique to transmit redundant packets to improve the latency performance, however, transmitting redundant packets will consume more energy. The algorithm with redundancy will make its energy efficiency worse than that of the algorithm without redundancy. In the wireless sensor network, we use the two parameters: the number of sensor nodes alive and the remaining energy to describe the energy efficiency.

When the remaining energy of a sensor node is lower than a certain threshold, the sensor is considered as "dead". In this tested, we choose 1.2×10^{-3} as the threshold. This threshold is the minimum energy to transfer a lK bits packets in a 1K bps bandwidth wireless channel. A sensor is "dead" means it cannot transmit/receive packets any longer, so it will be removed from the sensor network. The sensor is used to collect data and transmit the packets. The number of sensor of a

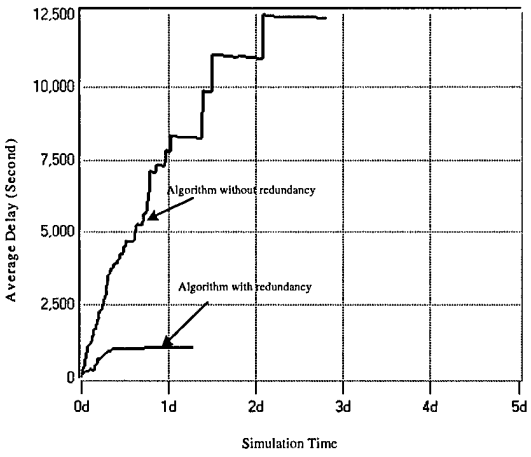


Fig. 3. Average latency performance of the two algorithms

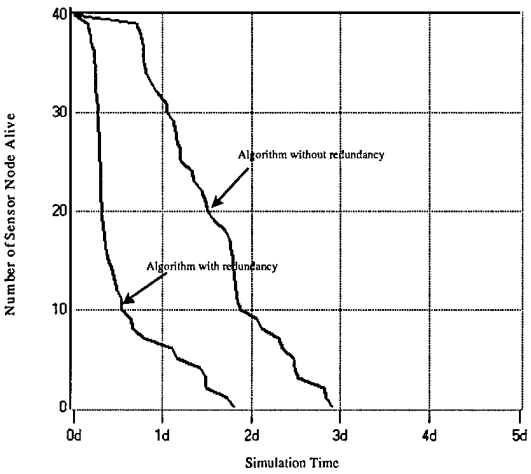


Fig. 4. Sensor nodes alive of the two algorithms

wireless sensor networks which is below a certain threshold means this network does not work. As Fig.4 shows, the remaining sensor nodes alive of the algorithm with redundancy for high priority packets are decreasing much quicker that of the algorithm without redundancy. As descried in the 2-Hop relay algorithm, we choose the sensors with most enegy as the destination; we can keep the energy consumption balance among sensors. We can observe from Fig.4 that the curve is dropping sharply. Comparing the average delay performance, we can find it is a tradeoff between system life and delay performance. The simulation result could be a reference when we design the wireless sensor network.

Fig.5 shows the remaining energy of the two scheduling algorithm. We assume that the energy of each sensor is 10J and the packet size is 125 bytes (1K bits), and the channel transmission rate is 1K bps. So when the sensor transmits or receives a packet, it will cost 1 second. And we adopt CSMA/CA protocol to solve the packets collision problem. If a sensor node transmits Num_s packets (each packet cost 1 second) and receives Num_r packets (each packets also cost 1

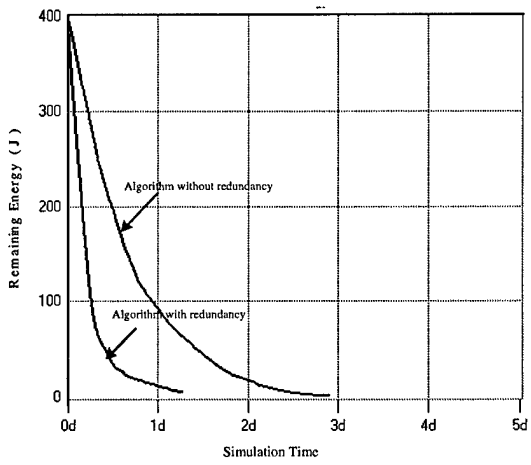


Fig. 5. Remaining energy of the two algorithms

second) and it is roaming in the network for T_m, we can get the remaining energy E_i of this sensor node:

$$E_i = 10-(3\times10^{-5}\times T_m+1.2\times10^{-3}\times1+6\times10^{-4}\times1) \quad (4)$$

The remaining energy E_w of the whole networks is described as:

$$E_w = \sum_{i=1}^{40} E_i \quad (5)$$

Figure 5 shows the remaining energy of the algorithm without redundancy is not dropping as sharply as that of the algorithm without redundancy. It illustrates that the algorithm without redundancy cost less energy.

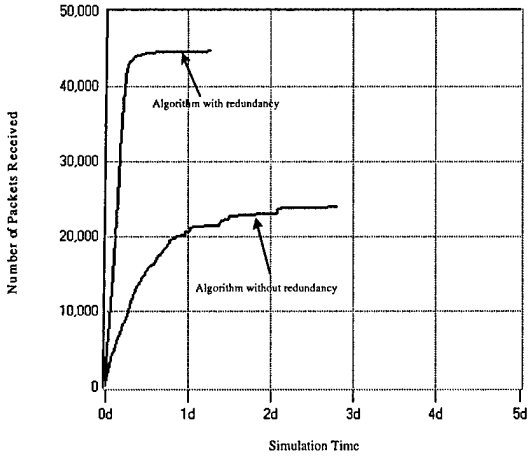


Fig. 6. Packets received of the two algorithms

3) Network quality: The role of the wireless sensor network in the real world is to collect data and transmit packets. In our simulation, we assume the collecting data distribution of the sensor node is Poisson distribution and the arriving interval is 1 second. Observing from Fig.6, although the lifetime of the algorithm with redundancy is shorter than that of the

algorithm without redundancy, but it can collect and transmit more packets. It is quite interesting. One of the main reasons is that the sensors in the networks are keeping moving, that means it keeps consuming energy. For the algorithm without redundancy, the sensor node consumes more energy under idle condition, although the sensor node of the algorithm with redundancy consumes more energy when it transmits or receives packets.

From Fig 5 to 6, we can observe that the simulation time of the algorithm with redundancy is shorter than that of the algorithm without redundancy, which means the networks lifetime of the algorithm with redundancy is shorter.

V. Conclusion

In order to meet different performance requirement of the service, we classified the services into high priority and low priority. Considering the effect of transmitting redundant packets, the 2-Hop relay algorithm was introduced. The algorithm with redundancy can improve the delay performance, but cost more energy to reduce the system life. We established the wireless sensor networks model as a cell partitioned structure, and sensor moves according to the one-step Markov path model with constant speed. The simulation result shows that the 2-Hop relay algorithm with/without redundancy can establish the delay/energy tradeoffs to meet different performance requirement of the services in WSN. Other parameters such as wireless channel bandwidth, degree of mobility and sensor density etc will also affect the delay/energy tradeoffs. It can be considered in the future work.

Acknowledgment

This work was supported by the U.S. Office of Naval Research (ONR) Young Investigator Award under Grant N00014-03-1-0466.

References

[1] Akyildiz, I. et al; " A survey on sensor networks ," *IEEE Coummun. Magazine*, pp.102-114, Aug. 2002

[2] Heinzelman, W.B.; Chandrakasan, A.P.; Balakrishnan, H.; " An application-specific protocol architecture for wireless microsensor networks ," *IEEE Transactions on Wireless Communications*, Volume: 1 Issue: 4, Oct 2002

[3] Neely, M.J.; Modiano, E.; " Capacity and delay tradeoffs for Ad-Hoc mobile networks ," *IEEE Transactions on the Procedding of Information theory*,

[4] Hou T. C.;Tsai T. J.; "Adaptive clustering in a hierarchical ad hoc network" *Proc. Int. Computer Symp.,Tainan, Taiwan,R.O.C.*, Dec.1998, pp.171-176.

[5] Nakano K.;Olariu S.; "Randomized initializtion protocols for Ad Hoc networks" *IEEE Transactions on Parallel and distributed systems,* , Vol.11, No.7, July 2000

[6] Lu, C. et al; " RAP: a real-time communication architecture for large-scale wirelss sensor networks ," *Proceeding of the eighth IEEE real-time and embedded technology and applications Symposium*, Sept. 2002, Pages:55-66

[7] Raghavendra, C.S.; Singh, S.; " PAMAS-Power aware multi-access protocol with signalling for Ad-Hoc networks," *Proceeding of the eighth IEEE real-time and embedded technology and applications Symposium*, 28-31 July 1998, Pages:310-321

[8] Grossglauser, M.;Tse, D.; " Mobility increases the capacity of Ad-hoc wireless networks ," *IEEE/ACM Transactions on Networking*, Volume: 10 , Issue: 4 , Aug. 2002, Pages:477 - 486

Latency and Energy Efficiency Evaluation in Wireless Sensor Networks

Xinsheng Xia
Department of Electrical Engineering
University of Texas at Arlington
416 Yates Street
Nedderman Hall, Rm 541
Arlington, TX 76010
Email: xia@wcn.uta.edu

Qilian Liang
Department of Electrical Engineering
University of Texas at Arlington
416 Yates Street
Nedderman Hall, Rm 541
Arlington, TX 76010
Email: liang@uta.edu

Abstract— **The performance evaluation is one the most important research topics for the Wireless Sensor Networks (WSN). Latency and energy efficiency are two important parameters to evaluate the WSN quality. To reduce delays in the WSN, the sensor node will send out redundant packets. Suppose the WSN has a cell-partitioned structure and the two-hop relay algorithm is adopted, the relay/destination nodes selection will determin the networks performance. The fuzzy logic system (FLS) is applied to the nodes selection and three descriptors are used: distance to the source node, the remaining energy and the degree of mobility. The output of FLS application provides a node election probability and we can elect three highest probability nodes as the relay nodes and in another FLS application, we choose the highest probability node as the destination. In contrast with the cases that only consider one descriptor, the FLS application can manage the delay/energy efficiency tradeoffs.**

I. Introduction

Wireless sensor networks are likely to be widely deployed in commercial and military applications. However, several obstacles need to be overcomed, such as latency-aware and energy efficiency [1] [2]. Latency-aware means to transfer the information among the sensors as quickly as possible. Energy efficiency means to the networks should function for as long as possible.

We adopt the cell-partitioned model in this paper (see Figure I): although the structure of cell regions is arbitrary, we still can assume that the network is divided into non-overlapping cells, each cell is of equal size [3].

The sensors are roaming independently from cell to cell. If two sensors are in the same cell, they can transfer packets with each other, and sensors within different cells cannot communicate. The sensors have a varaible mobility speed and actual mobility can be described by one-step Markov path model [4]. Each sensor can generate packets with a Poisson distribution and each sensor can reserve original packets and relay packets. Each packet enters its subqueue according to its destination node ID. This model can simplify the scheduling complexity and facilitates analysis. It can also conceal the detail of global network topology from the individual sensor node [6].

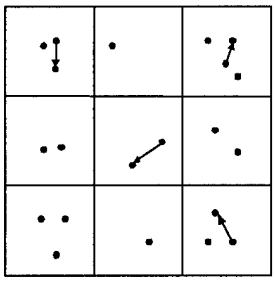


Fig. 1. A cell-partitioning wireless sensor network

In this paper [5], we consider the tradeoffs between the delay performance and the energy efficiency offered by the cell partitioned wireless model. We realized it with the two-hop relay algorithm. The FLS is used to elect the three relay nodes. When there are several pairs within one cell, we use the FLS to elect the destination node.

Generally, a node with the maximum remaining energy capacity or a node with the nearest distance to the source node or a node with the highest degree of mobility is elected as the relay/destination node. In this paper, we propose a scheme which make the nodes decision based on the following three descriptors:

1) distance of a node to the source node,
2) its remaining energy, and
3) its degree of mobility.

In order to evaluate the algorithm, we need to understand the major parameters about the wireless sensor network.

A. Latency

Because data communications in the sensor networks has trimming constraints, it is important to design the network algorithm to meet a kind of end-end deadlines [7].

B. System lifetime

It is not convenient to recharge the sensor node battery, so the energy efficiency is extremely important for sensor network. And the network should keep a enough number of

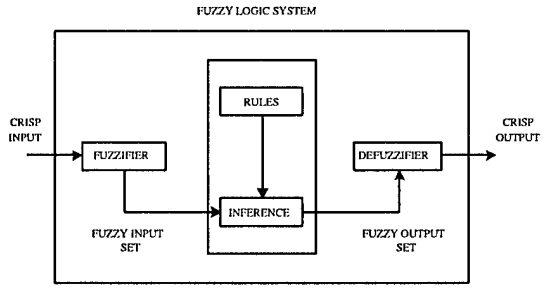


Fig. 2. The structure of a fuzzy logic system

"live" sensor nodes to collect data, that means the network need to keep the energy among the sensor nodes in balance. We use the remaining alive sensor nodes as the parameter of the networks lifetime.

C. Network efficiency

The sensor network is used to collect data and transfer packets. The amount of packets transmitted is one of the parameters to evaluate the networks efficiency.

II. Overview of Fuzzy Logic Systems

Figure II shows the structure of a fuzzy logic system(FLS).

When an input is applied to a FLS, the inference engine computes the output set corresponding to each rule. The defuzzifer then computes a crisp output from these rule output sets [8]. Consider a p-input 1-output FLS, using singleton fuzzification, *center-of-sets* defuzzification [9] and "IF-THEN" rules of the form [10]

$$R^l : \text{IF } x_1 \text{ is } \mathrm{F}_1^l \text{ and } x_2 \text{ is } \mathrm{F}_2^l \text{ and } \cdots \text{ and } x_p \text{ is } \mathrm{F}_p^l, \text{ THEN } y \text{ is } \mathrm{G}^l.$$

Assuming singleton fuzzification, when an input $\mathbf{x}' = \{x_1', \ldots, x_p'\}$ is applied, the degree of firing corresponding to the lth rule is computed as

$$\mu_{\mathrm{F}_1^l}(x_1') \star \mu_{\mathrm{F}_2^l}(x_2') \star \cdots \star \mu_{\mathrm{F}_p^l}(x_p') = \mathcal{T}_{i=1}^{p} \mu_{\mathrm{F}_i^l}(x_i') \quad (1)$$

where $\star$ and $\mathcal{T}$ both indicate the chosen t-norm. There are many kinds of defuzzifiers. In this paper, we focus, for illustrative purposes, on the center-of-sets defuzzifier. It computes a crisp output for the FLS by first computing the centroid, c_{G^l}, of every consequent set G^l, and, then computing a weighted average of these centroids. The weight corresponding to the lth rule consequent centroid is the degree of firing associated with the lth rule, $\mathcal{T}_{i=1}^{p} \mu_{\mathrm{F}_i^l}(x_i')$, so that

$$y_{cos}(\mathbf{x}') = \frac{\sum_{l=1}^{M} c_{\mathrm{G}^l} \mathcal{T}_{i=1}^{p} \mu_{\mathrm{F}_i^l}(x_i')}{\sum_{l=1}^{M} \mathcal{T}_{i=1}^{p} \mu_{\mathrm{F}_i^l}(x_i')} \quad (2)$$

where M is the number of rules in the FLS.

In this paper, we design a FLS for relay/destination nodes election. The rules are designed based on the knowledge from a group of network experts.

III. Energy,Delay,And The 2-Hop Relay Algorithm

A. Energy

A sensor node consumes significant energy when it transmits or receives a packet. It will also consume energy when the sensor node is idle. The power consumption ratio: Transmit: receive: idle of the sensor node is approximately: 40:20:1 [11].

The distance between two nodes are variable in the WSN and the power loss model is used. To send the packet, the sender consumes,

$$P_{tx} = P_{elec} + \epsilon_{fs} \cdot d^2 \quad (3)$$

and to receive the packet, the receiver consumes,

$$P_{rx} = P_{elec} \quad (4)$$

where P_{elec} represents the power that is necessary for digital processing, modulation, and ϵ_{fs} represents the power dissipated in the amplifier for the free space distance d transmission.

B. Delay

The packet transmission latency between the sensors includes three parts: the wireless channel transmission delay, the Physical/Mac layer transmission delay, and the queuing delay.

Defined D as the distance between two sensors and C as the light speed, the wireless channel transmission delay as:

$$Delay_{ch} = \frac{D}{C} \quad (5)$$

The Physical/Mac layer transmission delay will be decided by interaction of the transmitter and the receive channel, the sensor density and the sensor traffic intensity etc.

The queuing delay is decided by the sensor I/O system processing rate, the subqueue length in the sensor, the probability that a source-destination pair meeting within one cell and the degree of mobility. The higher degree of mobility, the lower transmission delay.

In order to make the system"stable", the rate at which sensor node transfers packets intended for its destination must satisfy all sensor that the queuing lengths will not be infinite and the average delays will be bounded.

C. The two-Hop Relay Algorithm

This relay algorithm restricts packets to 2-hop paths, and the relay packet is inserted into the subqueue of the relay sensors until a source encounters its destination.

Two-hop Relay algorithm [12]:

1)If there exists source-destination pairs within the cell, there are two options:

- If there exists one source-destination pair within the cell and if the source contains a new packet intended for that destination, transmit it.
- If there exists more than one source-destination pair within the cell, choose the sensor with the longest subsequeue as the source and choose one sensor as the destination and transmit it.

2)If there is no source-destination pair in the cell, there are two options:

- Send a Relay packet to its destination: if the designated transmitter has a packet destined for the designated receiver, send that packets to the receiver.
- Send a new relay packet: if the designated transmitter has a new packet that has never before been transmitted, conserve the packet in his own subqueue according to its destination. Choosing the three sensors as the relay destinations and transmit three copies to them.

This algorithm restricts all routes to 2-hop while the relay packets are only allowed to transmit to their destinations. We pick up the packet reserved in the subqueue with the longest queuing length to keep the queuing length in balance among the sensors in order to reduce the time jitter.

When the networks transmit a packet, it will schedule with redundancy. Transmitting/receiving redundancy can improve delay, it will also cause more energy consumption. When we use the algorithm in the wireless sensor networks, more complications arise. We proposed more scheduling algorithms to overcome these complications.

D. Cell location algorithm

Each sensor node knows its location (X position, Y position). As all the cells are the same size, each sensor node can determine the cell serial number it belongs to.

For example, the network size is $N \times N$ and it is partitioned into $C = S^2$ cells:

$$Cell_{sn} = [\frac{X \cdot S}{N}] + [\frac{Y \cdot S}{N}] \cdot S + 1 \qquad (6)$$

Where [ ] refer to the round function, the round function will round the value of the float argument to the nearest integer value.

Every sensor will send a "Hello" message with its cell serial number $Cell_{sn}$ and other information to other sensors between a constant time interval. When a sensor with ID number A receives a "Hello" message sent by sensor B. Sensor A compares its cell serial number $Cell_{sna}$ with the cell serial number $Cell_{snb}$ of sensor B.

- If $Cell_{sna}$ is equal to $Cell_{snb}$, that means sensor A and sensor B are in the same cell and the information of sensor B already in the database of sensor A, update the information of sensor B.
- If $Cell_{sna}$ is equal to $Cell_{snb}$, that means sensor A and sensor B are in the same cell but the information of sensor B is not in the database of sensor A, record the information of sensor B.
- If $Cell_{sna}$ not equal to $Cell_{snb}$, that means sensor A and sensor B are not in the same cell but the information of sensor B is in the database of sensor A, delete the information of sensor B.
- If $Cell_{sna}$ not euqal to $Cell_{snb}$, that means sensor A and sensor B are in the same cell but the information of sensor B is not in the database of sensor A, remain idle.

Notice that a sensor only keeps the information of the sensors that in the same cell and keeps updating it, the sensor can reduce the memory usage and keep the latest information.

E. In-cell feedback algorithm

As there is redundancy in the network, when a packet has been delivered to its destination, its remnant versions of this packet should be removed from the network. We assume all packets have a send serials number SN. SN combined with source sensor ID is unique in the network. When a sensor node A receive a packet, it will send out a "notice" message with its SN $Packet_{sn}$, source sensor ID B and destination sensor ID A.

When a sensor receive the "notice" message, it will search packet with SN in the A subqueue. If there is a packet with SN $Packet_{sn}$, source sensor ID B and destination sensor ID A, remove it from the subqueue. Otherwise, remain idle.

Notice that, no packet will transmit to its destination twice. So we can reduce the energy consumption and shorten average delay.

IV. The FLS application for the two-hop relay algorithm

The effect of transmitting redundant packets will consume more energy, however, it will also increase the chance that the nodes which hold the original or relay packets to reach their destination. How to elect the relay nodes or when there are several pairs nodes within one cell, how to elect the node as the destination will determine the energy and latency performance.

We collect the knowledge for nodes election based on the following three descriptors:

1) distance of a node to the source node,
2) its remaining energy, and
3) its degree of mobility.

The linguistic variables used to represent the distance of a node to the source node were divided into three levels: *near*, *moderate*, and *far*; and those to represent its remaining energy and degree of mobility were divided into three levels: *low*, *moderate*, and *high*. The consequent – the possibility that this node will be elected as a relay/destination node – was divided into 5 levels, *Very Strong, Strong, Medium, Weak, Very Weak.*

We designed questions such as:

> IF *distance of a node to the source node* is *near*, and *its remaining energy* is *low*, and *its degree of mobility* is *moderate*, THEN the possibility that this node will be elected as a relay/destination is _____.

so we need to set up $3^3 = 27$ (because every antecedent has 3 fuzzy sub-sets, and there are 3 antecedents) rules for this FLS.

We created one survey for the network experts. We used rules obtained from the knowledge of 6 network experts. These experts were requested to choose a consequent using one of the five linguistic variables. Different experts gave different answers to the questions in the survey. Table I summarizes

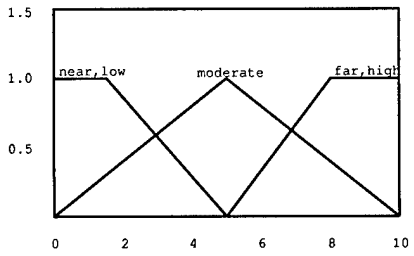


Fig. 3. MFs for antecedents

the questions used in this survey, and Table II captures the results from the completed survey.

We used trapezoidal membership functions (MFs) to represent *near*, *low*, *far*, and *high*, and triangle MFs to represent *moderate*. We show these MFs in Fig.III.

In our approach to forming a rule base, we chose a single consequent for each rule. To do this, we averaged the centroids of all the responses for each rule and used this average in place of the rule consequent centroid. Doing this leads to rules that have the following form:

R^l : IF *distance of a node to the source node* (x_1) is F_l^1, and *its remaining energy* (x_2) is F_l^2, and *its degree of mobility* (x_3) is F_l^3, THEN the possibility that this node will be elected as a relay/destination (y) is c_{avg}^l.

where $l = 1, \ldots, 27$. c_{avg}^l is defined as

$$c_{avg}^l = \frac{\sum_{i=1}^{5} w_i^l c^i}{\sum_{i=1}^{5} w_i^l} \tag{7}$$

in which w_i^l is the number of people choosing linguistic label i for the consequent of rule l ($i = 1, \cdots, 5; l = 1, \ldots, 27$) (see Table II); and, c^i is the centroid of the ith consequent set ($i = 1, 2, \cdots, 5$). The centroids of the three fuzzy sets depicted in Fig. IV are $c^1 = 1.0561$, $c^2 = 3$, $c^3 = 5$, $c^4 = 7$, and $c^5 = 8.9439$.

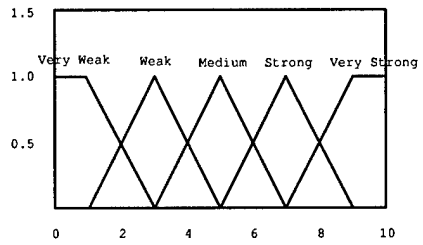


Fig. 4. MFs for consequent

To illustrate the use of (7), note, for example, that

$$c_{avg}^{11} = \frac{3c^1 + 2c^2 + c^3}{3 + 2 + 1} = 2.3614 \tag{8}$$

All 27 c_{avg}^l values are listed in Table II.

For every input (x_1, x_2, x_3), the output is computed using

$$y(x_1, x_2, x_3) = \frac{\sum_{l=1}^{27} \mu_{\mathrm{F}_l^1}(x_1)\mu_{\mathrm{F}_l^2}(x_2)\mu_{\mathrm{F}_l^3}(x_3)c_{avg}^l}{\sum_{l=1}^{27} \mu_{\mathrm{F}_l^1}(x_1)\mu_{\mathrm{F}_l^2}(x_2)\mu_{\mathrm{F}_l^3}(x_3)} \tag{9}$$

V. Simulation

We used the OPNET modeler to implement the simulation model. The simulation region is 180×180 meters, and it was divided into 9 non-overlapping cells. Each cell is of equal size, that is 60×60 meters. In the previous section, we know that the power consumption ratio is 40:20:1. So we can assume that the sensor node consumes approximately 3×10^{-5} watts when idle, 1.2×10^{-3} watts during transmission and 6×10^{-4} watts during reception. As we adopted the path loss model, 1.2×10^{-3} watts is the maximum value for transmission.

There are 80 sensor nodes in the simulation model, and the sensors are roaming independently with the ground speed from 1 m/s to 9 m/s. The mobility model is called one-step Markov path model. The probability of moving in the same direction as the previous move is higher than other directions in this model; it means this model has memory. Fig. V shows the probability of the six directions.

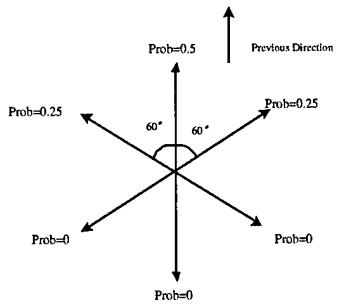


Fig. 5. One-step Markov path model

In the testbed, we use the average latency (see equation 10.)to evaluate the network performance. Every packet was labeled a timestamp when it was generate by the source sensor node. When the packet reaches its destination, the time interval is the transmission delay.

$$Average\ Latency = \frac{\sum_{i=1}^{K} D_i}{K} \tag{10}$$

When the remaining energy of a sensor node is lower than a certain threshold, the sensor is considered as"dead". In this testbed, we choose 1.2×10^{-3} as the threshold. This threshold is the energy which can be used to transfer a 1 K bits packets in a 1K bps bandwidth wireless channel. A sensor is "dead" means it cannot transmit/receive packets any longer, so it will be removed from the sensor network.

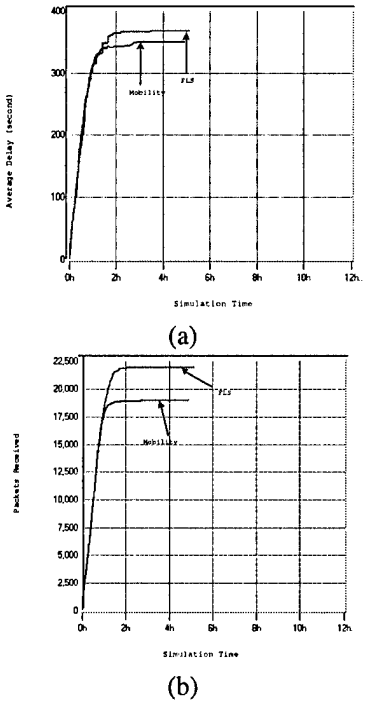
We assumed that the energy of each sensor is 5J and the packet size is 125 bytes (1K bits), and the channel transmission rate 1k bps. So when the sensor transmit or receive a packet, it will cost 1 second. If a sensor transmitted one packet, received one packet, and it is roaming in the network for T_m seconds,

we can get the remaining energy E_i of this sensor node in Equation 11:

$$E_i = 5-(3\times10^{-5}\times T_m+(6\times10^{-4}+8.33\times10^{-7}\times d^2)\times1+6\times10^{-4}\times1) \quad (11)$$

A. FLS vs Mobility

We obtained the simulation result of FLS application which considered three antecedents. If we only consider one antecedent: the degree of mobility, the performance of average delay will be better. As plotted in Fig. 6(a), the performance of average delay which only considered the degree of mobility was about 5% better than that of FLS application. However, the FLS application can achieved a better performance for packets received, about 10%, as plotted in Fig. 6(b).



(a)

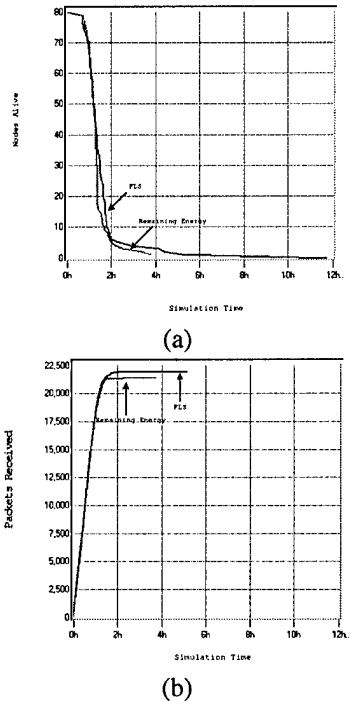
(b)

Fig. 6. The FLS application vs the degree of mobility. (a) average delay, and (b) packets received.

B. FLS vs the Remaining Energy

Similarly, we only consider one antecedent: the remaining energy, the performance of first "dead" node will be better. As plotted in Fig. 7(a), the life time of the first "dead" node was 3 minute longer than that of FLS application. However, the FLS application achieved a better performance for the network life, about 8 hours longer. The reason is that we adopted the path loss model in the testbed and the FLS has considered another antecedent: the distance to the source node. The nearer distance, less energy consuming. The FLS application also achieved a better performance for the packets received, about 5%, as plotted in Fig. 7(b).

Simulation results show that the FLS application can manage the delay/energy tradeoffs. If we design different FLS



(a)

(b)

Fig. 7. The FLS application vs the remaining energy. (a) nodes alive, and (b) packets received.

in the two-hop relay algorithm, we could meet different performance requirement in WSN.

VI. Conclusion

In the two-hop relay algorithm, the relay nodes election or when there are several pairs of sensor nodes within one cell, the destination node election will determin the network performance. We apply the fuzzy logic system (FLS) to the relay/destination nodes selection. Three descriptors are used: the distance to the source node, the remaining energy and the degree of mobility. We obtained the linguistic knowledge from a group of experts. Based on the linguistic knowledge, we set up 27 rules. The nodes possibility is the output of FLS. We elected the nodes with the highest three possibilities as the relay nodes while we elected the FLS to elect the node with the highest possibility as the destination node. Further more, simulation results suggest that the FLS application in the two-Hop relay algorithm could manage the delay/energy efficiency tradoffs.

Acknowledgment

This work was supported by the Office of Naval Research (ONR) Young Investigator Award under Grant N00014-03-1-0466.

References

[1] Akyildiz, I. et al; " A survey on sensor networks ," *IEEE Coummun. Magazine*, pp.102-114, Aug. 2002

[2] Heinzelman, W.B.; Chandrakasan, A.P.; Balakrishnan, H.; " An application-specific protocol architecture for wireless microsensor networks ," *Wireless Communications, IEEE Transactions on*, Volume: 1 Issue: 4, Oct 2002

[3] Neely, M.J.; Modiano, E.; " Capacity and delay tradeoffs for Ad-Hoc mobile networks ," *Procedding of Information theory, IEEE Transactions on*,

[4] Hou T. C.;Tsai T. J.; "Adaptive clustering in a hierarchical ad hoc network" *Proc. Int. Computer Symp.,Tainan, Taiwan,R.O.C.*, Dec.1998, pp.171-176.,

[5] Xia, X.;Liang, Q.; "Latency-aware and energy efficiency tradeoffs for sensor networks" *Submitted to Personal, Indoor and Mobile Radio Communications, 2004. PIMRC 2004. 15th IEEE* ,

[6] Nakano K.;Olariu S.; "Randomized initializtion protocols for Ad Hoc networks" *Parallel and distributed systems, IEEE Transactions on*, Vol.11, No.7, July 2000,

[7] Lu, C. et al; " RAP: a real-time communication architecture for large-scale wirelss sensor networks ," *Proceeding of the eighth IEEE real-time and embedded technology and applications Symposium*

[8] Liang,Q.; "Clusterhead election for mobile ad hoc wireless network" *Personal, Indoor and Mobile Radio Communications, 2003. PIMRC 2003. 14th IEEE*, Proceedings on ,Volume: 2 , Sept. 7-10, 2003 Pages:1623 - 1628,

[9] Mendel,J. M.; *Uncertain Rule-Based Fuzzy Logic Systems*, Prentice-Hall, Upper Saddle River, NJ, 2001.

[10] Mamdani,E. H.; " Applications of fuzzy logic to approximate reasoning using linguistic systems", *IEEE Trans. on Systems, Man, and Cybernetics*, vol. 26, no. 12, pp. 1182-1191, 1977.

[11] Raghavendra,C.S.; Singh, S.; " PAMAS-Power aware multi-acess protocol with signalling for Ad-Hoc networks," *Proceeding of the eighth IEEE real-time and embedded technology and applications Symposium*,

[12] Grossglauser, M.;Tse, D.; " Mobility increases the capacity of Ad-hoc wireless networks ," *Networking, IEEE/ACM Transactions on* ,, Volume: 10 , Issue: 4 , Aug. 2002, Pages:477 - 486

TABLE I

THE QUESTIONS FOR NODES ELECTION FOR THE TWO-HOP RELAY ALGORITHM. ANTECEDENT 1 IS *distance of a node to the source node*, ANTECEDENT 2 IS *its remaining energy*, ANTECEDENT 3 IS *its degree of mobility*, AND CONSEQUENT IS *the possibility that this node will be elected*. THE EXPERTS WERE ASKED TO FILL IN THE BLANK FOR THE CONSEQUENT USING ONE OF FIVE LINGUISTIC LABELS (VERY WEAK, WEAK, MEDIUM, STRONG, VERY STRONG).

Question #	Antecedent 1	Antecedent 2	Antecedent 3	Consequent
1	near	low	high	
2	near	low	moderate	
3	near	low	low	
4	near	moderate	high	
5	near	moderate	moderate	
6	near	moderate	low	
7	near	high	high	
8	near	high	moderate	
9	near	high	low	
10	moderate	low	high	
11	moderate	low	moderate	
12	moderate	low	low	
13	moderate	moderate	high	
14	moderate	moderate	moderate	
15	moderate	moderate	low	
16	moderate	high	high	
17	moderate	high	moderate	
18	moderate	high	low	
19	far	low	high	
20	far	low	moderate	
21	far	low	low	
22	far	moderate	high	
23	far	moderate	moderate	
24	far	moderate	low	
25	far	high	high	
26	far	high	moderate	
27	far	high	low	

TABLE II

HISTOGRAMS OF EXPERT RESPONSES ABOUT NODES ELECTION FOR THE TWO-HOP RELAY ALGORITHM. 6 NETWORK EXPERTS ANSWERED THE QUESTIONS. THE ENTRIES IN THE SECOND – SIXTH COLUMNS CORRESPOND TO THE WEIGHTS w_1^l, w_2^l, w_3^l, w_4^l, AND w_5^l, RESPECTIVELY.

Rule # (l)	very weak	weak	medium	strong	very strong	c_{avg}^l
1	0	3	3	0	0	4.0
2	1	5	0	0	0	2.676
3	3	1	2	0	0	2.6947
4	0	0	3	3	0	6.0
5	0	0	0	5	1	7.3240
6	0	4	1	1	0	4.0
7	0	0	0	1	5	8.6199
8	0	0	1	5	0	6.6667
9	0	1	4	1	0	5.0
10	0	4	2	0	0	3.6667
11	3	2	1	0	0	2.3614
12	4	1	1	0	0	2.0374
13	0	1	3	2	0	5.3333
14	1	1	4	0	0	4.0093
15	2	3	0	1	0	3.0187
16	0	0	2	3	1	6.6573
17	0	1	2	3	0	5.6667
18	0	3	2	1	0	4.3333
19	2	4	0	0	0	2.3520
20	5	1	0	0	0	1.3801
21	5	1	0	0	0	1.3801
22	1	4	1	0	0	3.0093
23	1	4	1	0	0	3.0093
24	5	0	1	0	0	1.7134
25	0	2	2	2	0	5.0
26	0	0	2	3	1	6.6573
27	0	2	2	1	1	5.3240

Sensor Placement and Lifetime of Wireless Sensor Networks: Theory and Performance Analysis

Ekta Jain and Qilian Liang
Department of Electrical Engineering
University of Texas at Arlington
Arlington, TX 76019-0016 USA
E-mail: jain@wcn.uta.edu, liang@uta.edu

Abstract— **Increasing the lifetime of energy constrained wireless sensor networks is one of the key challenges in sensor network research. In this paper we present a *bottom-up* approach to evaluating the lifetime performance of networks employing two basic sensor placement schemes: square-grid and hex-grid. Lifetimes of individual sensor node as well lifetimes of networks are modeled as random variables and their probability density functions (pdf) are obtained theoretically. Reliability theory is used for the network lifetime analysis, and provides a methodology for similar studies. Simulation results show that the actual pdf's match very closely to those obtained theoretically. The theoretical results provided in this paper will serve as a basis for other related research such as analysis of other sensor placement schemes, lifetime and sensor density tradeoff study, and performance of energy efficiency related algorithms.**

I. Introduction

Sensor networks represent a significant advancement over traditional invasive methods of monitoring and are more economical for long term data collection and monitoring when compared to the traditional personnel-rich methods. Although most military applications require random deployment of sensor nodes, a number of non-military applications allow the explicit placement of sensors at specific locations as desired. Such placement-friendly sensor networks are widely used for infrastructure security, environment and habitat monitoring, traffic control etc. [1]. An in-depth study of a real-world 32 node habitat monitoring sensor network system, which is deployed on a small island off the coast of Maine and studies nesting patterns of petrels has been presented in [6]. Another such application [5] involves the use of sensors in buildings for environmental monitoring which may include chemical sensing and detection of moisture problems. Structural monitoring [7] and inventory control are some other applications of such networks.

Wireless sensor networks comprise of small, energy constrained sensor nodes, which basically consist of single or multiple sensor modules, wireless transmitter-receiver modules, computational modules, and power supply module. These networks are usually employed to collect data from environments where human intervention after deployment, to recharge or replace node batteries may not be feasible, resulting in limited network lifetime. Most applications have pre-specified lifetime requirements, for instance the application in [6] has a lifetime requirement of at least 9 months. Thus estimation of lifetime of such networks prior to deployment becomes a necessity. Prior works on evaluation of lifetime have considered networks where sensor nodes are randomly deployed. [4] gives the upper bound on lifetime that any network with the specified number of randomly deployed nodes, source behavior and energy can reach while [3] discusses the upper bounds on lifetime of networks with cooperative cell based strategies.

In this paper we deal with the issues of sensor placement and lifetime estimation. We present a *bottom-up* approach to lifetime evaluation of a network. As a first step in this direction we investigate the lifetime behavior of a single sensor node and then attempt to apply this knowledge to arrive at the network lifetime behavior for two basic placement schemes. We believe that these simple schemes can serve as basis for evaluation of more complex schemes for their lifetime performance prior to deployment and help justify their deployment costs. We remark that our investigation can be applied to a network employing any routing protocol, and energy consumption scheme. Although in a less direct way, our analysis can also be used to assess various energy efficiency related algorithms for their lifetime performance. Also, since our analysis incorporates lifetime evaluation for minimum as well as high density placement, the tradeoff between cost of deployment and lifetime can be studied because higher density implies higher cost. Our analytical results are based on the application of reliability theory. These results are supported by extensive simulations, which validate our analysis.

This paper is organized as follows. Section II details the model used for this study and provides basic discussions on coverage, connectivity and lifetime. Section III describes the lifetime analysis of a single node and Section IV uses reliability theory to apply node lifetime analysis to network

lifetime analyses. Simulation and discussion of the key results of this work is presented in Section V, and Section VI concludes this paper.

II. Preliminaries

A. Basic Model

Consider identical wireless sensor nodes placed in a square sensor field of area A. All nodes are deployed with equal energy. Each sensor is capable of sensing events up to a radius of r_s, the sensing range. We also define a communication range r_c, beyond which the transmitted signal is received with signal to noise ratio (SNR) below the acceptable threshold level. We assume the communication range r_c to be equal to the sensing range r_s. The communication range depends on the transmission power level, gains of the transmitting and receiving antennae, interference between neighboring nodes, path loss, shadowing, multi path effects etc. Direct communication between two sensor nodes is possible only if their distance of separation r is such that $r \leq r_c$. We call such nodes *neighbors*. Communication between a sensor node and its non-neighboring node is achieved via peer-to-peer communication. Thus the maximum allowable distance between two nodes who wish to communicate directly is $r_{max} = r_c = r_s$. A network is said to be deployed with minimum density when the distance between its neighboring nodes is $r = r_{max}$.

B. Placement Schemes

The simplest placement schemes are those in which each node has the same number of neighbors. We arrive at two basic placement schemes by considering cases where each sensor nodes has four and three neighbors, arriving at the *square-grid* and *hex-grid* placement schemes shown in Fig1(a) and (b) respectively. A sensor node placement scheme that uses two neighbors per sensor node has been described in [2]. We believe that these three elementary placement schemes can serve as basis for other placement schemes, because a placement scheme of any complexity can be decomposed into two-neighbor, three-neighbor and four-neighbor groups. Both grids have the same number of nodes[1] and nodes in both grids are equidistant from their respective neighbors (with distance of separation r.)

C. Coverage and Connectivity

A discussion on coverage and connectivity becomes imperative before the lifetime of the network can be defined. Coverage scales the adequacy with which the network covers the sensor field. A sensor with sensing range r_s is said to cover a circular region of radius r_s around it.

[1]The *Hex-grid* has lower density than the *Square-grid*. With 36 nodes deployed, the network with *Square-grid* covers an area of $25r^2$, and the *Hex-grid* covers an area of $48r^2$, almost double that of the *square grid*.

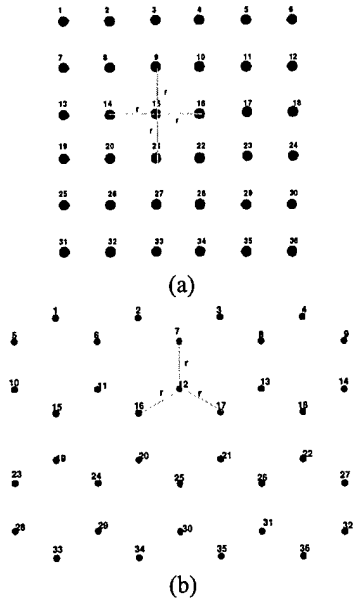


Fig. 1. Placement Schemes for a 36 node sensor network: (a) Square-Grid (b) Hex-Grid.

If every point in the sensor field is within distance r_s from at least one sensor node, then the network is said to provide complete coverage. Various levels of coverage may be acceptable depending on the application. In critical applications complete coverage may be required at all times, and the first loss of coverage may lead to failure of the network. In some other applications a small loss of coverage may be acceptable. An example of a sensor placement scheme that concentrates mainly on coverage as its parameter of interest can be found in [9]. In our analysis we require the network to provide complete coverage.

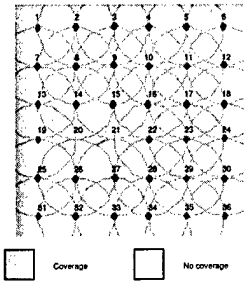
Connectivity scales the adequacy with which the nodes are able to communicate. If a large number of nodes fail due to lack of energy, a part of the network may get completely disconnected from the rest. In our analysis we assume that only 100% connectivity is acceptable. The network fails with loss of connectivity.

D. Lifetime

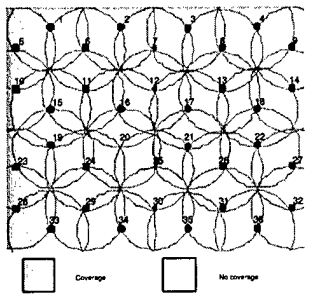
Lifetime is the post-deployment active time period of the network and is defined as the time to first loss of connectivity or coverage. This definition corresponds to the minimum lifetime or the worst case scenario. The number of node failures that a given network can tolerate without failing itself depends on the placement scheme employed and its density . If the minimum number of node failures that can cause network failure can be found, then the minimum network lifetime can be estimated. Although our analysis is valid for any definition of lifetime specifying

a certain number of node failures required for network failure, we limit our analysis to the minimum network lifetime.

1) Minimum Density Networks: Consider the square-grid and the hex-grid deployed with minimum density. Both schemes tolerate the failure of a node all of whose neighbors are functioning, without loss of either connectivity or coverage. Thus a single node failure does not cause network failure. Failure of two or more neighboring nodes causes loss of coverage and hence network failure as indicated in Figs 2(a) and (b). A network may undergo multiple node failures and still be connected and covered if the failed nodes are not adjacent to each other. But the minimum number of node failures that cause network failure is two. Therefore we define the minimum network lifetime for the square-grid and the hex-grid as the time to failure of any two neighboring nodes, i.e., the first loss of coverage.



(a)



(b)

Fig. 2. Loss of coverage due to failure of two neighboring nodes: (a)Square-grid: Failure of nodes 20 and 21 causes loss of coverage. (b)Hex-grid: Failure of nodes 20 and 25 causes loss of coverage.

2) Network lifetime for dense placement: If $r < r_{max}$, then a node may be able to communicate not only with the nodes immediately adjacent to it, but also with other nodes which fall in its range. The number of nodes deployed (N), corresponding to r are higher than the minimum number of nodes required (N_{min}) corresponding to $r = r_{max}$. We discussed earlier that the minimum lifetime of a square-grid or hex-grid network with $r = r_{max}$(minimum density) is the time to failure of two neighboring nodes. For dense networks the network can lose $N - N_{min}$ nodes and still be deployed with minimum density. Thus it needs two neighboring node failures after $N - N_{min}$ node failures to lose coverage or connectivity. The first loss of connectivity or coverage for dense network corresponds to $(N - N_{min} + 2)$ node failures. This kind of a network is modeled in Section IV-C.

III. Node Lifetime Evaluation

We begin our analysis with the estimation of the lifetime of a single sensor node. A node is said to have m possible modes of operation, and at any given time the node is in one of these m modes. Let w_i be the fraction of time that a node spends in the i^{th} mode, where w_i's are such that,

$$\sum_i w_i = 1 \;\; i = 1, 2...m \tag{1}$$

The w_i's do not remain constant in general and may vary for different networks scenario's. Hence they are modeled as random variables that take values from 0 to 1 according to a specific probability distribution function (*pdf*) which we attempt to find.

We assume that the total energy at the time of deployment is E_{total} and that the node spends a power of P_i watts/unit time, while in the i^{th} mode. If T_{node} is the lifetime of the node, then the node spends $w_i T_{node}$ time units in mode i. We define the lifetime of a node as the time from deployment to when its energy drops below a threshold energy value E_{th}. The following equation follows from this definition.

$$\begin{aligned} E_{total} - \sum_i w_i P_i T_{node} &\geq E_{th} \\ T_{node} &\geq \frac{E_{total}}{\sum_i w_i P_i} \end{aligned} \tag{2}$$

We observe from this equation that T_{node} is a function of the random variables w_i and hence is a random variable itself. This is an important observation as it implies that since the modes of the various nodes cannot be known *a priori*, the lifetime of a single node can be best represented as a random variable that takes different values with certain probabilities defined by its probability density function (*pdf*) $f_t(t)$. In order to obtain the *pdf* of T_{node}, we first find the *pdf* of $w_i \, \forall i$.

To this purpose we assume that at any given time a node can be in one of its two modes of operation, *active* or *idle*. A node is *active* when it is either transmitting or receiving and is *idle* otherwise. If p is the probability of node being active, $1 - p$ is the probability of the node being idle at any given time.

$$Pr\{\text{node is active}\} = p \quad (3)$$

$$Pr\{\text{node is idle}\} = 1-p \quad (4)$$

Note that the actual values of p will depend on the protocol or the energy consumption scheme used. Let w_1 and w_2 be the fraction of time the node is in active and idle mode respectively. Since we assume only two modes of operation, $w_2 = 1 - w_1$. The random variable w_1 is clearly binomial in nature, with probability of success, i.e., probability of node in active mode being p. We observe the node over T time units. Since w_1 has a binomial distribution, the probability of the node being active for x time units of a total of T time units is give by,

$$P\{w_1 = x\} = C_T^x p^x (1-p)^{T-x} \quad (5)$$

As T becomes large, the binomial distribution can be approximated to a normal distribution with mean $\mu = Tp$ and variance $\sigma^2 = np(1-p)$. Since $w_2 = 1 - w_1$, w_2 also follows normal distribution with mean $\mu = T(1-p)$ and variance $\sigma^2 = np(1-p)$. Hence we conclude that the fraction of time that the node spends in any mode follows the normal distribution.

We observe from equation (2) that the denominator of the expression is a normal random variable because it is the sum of m normal random variables. This helps us draw an important conclusion that the reciprocal of the lifetime of a node is normally distributed.

IV. Network Lifetime Analysis using Reliability Theory

We are now ready to evaluate the network lifetime. Since the lifetimes of individual nodes are not constants but random variables, it follows that the network lifetime is also a random variable. We apply reliability theory to find the distribution of the network lifetime, given the node lifetime distribution. The following section treats the basics of reliability theory before going on to its application.

A. Reliability Theory

Reliability theory is concerned with the duration of the useful life of components and systems of components [10] [8]. We model the lifetime (of individual nodes and the network) as a continuous non-negative random variable T. The distribution of the random variable T can be represented in the following different ways.

1) Probability Density Function (pdf): The *pdf* gives the probability of the random variable taking a certain value. It is represented as $f(t)$ and has a probabilistic interpretation

$$f(t)\Delta t = P[t \le T \le t + \Delta t] \quad (6)$$

for small values of Δt. All *pdf*'s must satisfy two conditions, $\int_0^\infty f(t)dt = 1$ and $f(t) \ge 0, \forall t$. We have the distribution of the lifetime of a node in the form of its *pdf*, in that we know that the reciprocal of the node lifetime has a normal *pdf*.

2) Cumulative Distribution Function (cdf): The *cdf* corresponding to the *pdf* $f(t)$ is denoted by $F(t)$ and is very useful as it gives the probability that a randomly selected component or system will fail by time t. It can be expressed in three different ways:

- $F(t)$ = the area under the *pdf* $f(t)$ to the left of t.
- $F(t)$= the probability that a single randomly chosen new component will fail by time t.
- $F(t)$= the proportion of the entire population that fails by time t.

The relationship between the *cdf* and *pdf* of a random variable is given below:

$$F(t) = \int_0^t f(s)ds \quad (7)$$

3) Survivor Function: The *Survivor function* $S(t)$, also known as the *Reliability function* $R(t)$ is defined as the probability that a unit is functioning at any time t:

$$S(t) = P[T \ge t] \quad t \ge 0 \quad (8)$$

Since a unit either fails, or survives, and one of these two mutually exclusive alternatives must occur, we have,

$$S(t) = 1 - F(t) = 1 - \int_0^t f(s)ds \quad (9)$$

All survivor functions must satisfy three conditions: $S(0) = 1$, $\lim_{t\to\infty} S(t) = 0$, and $S(t)$ is non increasing.

4) System Reliability: The main objective of system reliability is the construction of a distribution that represents the lifetime of a system based on the lifetime distributions of the components from which it is composed. To accomplish this we consider the relationship between components. This approach to finding system lifetime has the inherent advantage that it is often easier and cost-effective to extensively test a single component or subsystem rather the whole system.

5) Reliability Block Diagram: Reliability block diagram (*RBD*) is a graphical representation of the components of the system, and provides a visual representation of the way components are reliability-wise connected. Thus the effect of the success or failure of a component on the system performance can be evaluated. For example, if one component failure of a bi-component system causes system failure, then we can conclude that the component blocks are connected in series in the *RBD*. Similarly if a bi-component system is said to fail only when both its components fail, then the component blocks are connected in parallel in the system *RBD*. If $S_1(t)$ and $S_2(t)$ are the

survival functions of two components of a bi-component system, then the system reliability for both cases is given as follow:

$$S_{series}(t) = S_1(t)S_2(t) \quad (10)$$
$$S_{parallel}(t) = 1 - [(1 - S_1(t))(1 - S_2(t))] \quad (11)$$

Any complex system can be realized in the form of a combination of blocks connected in series and parallel, and the system survival function can be obtained by using equations (10) and (11). In our analysis, the network is the system under consideration and the sensor nodes are the components of the system. All sensor nodes are assumed to have the same survival function since they are identical. They are also assumed to fail independent of one another.

B. Lifetime of minimum density networks

1) Square Grid: As defined in Section II-D.1, the minimum network lifetime is the time to failure of two adjacent nodes. Using this definition we build the RBD for the square-grid as shown in figure 3.

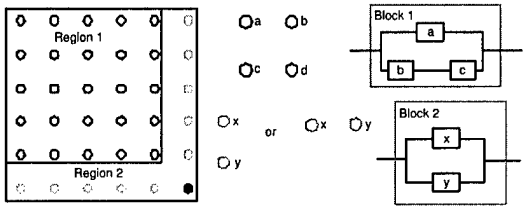


Fig. 3. RBD for square grid: RBD of a single node in a square grid. Nodes belonging to region-1 are modeled as block-1 and nodes belonging to region-2 are modeled as block-2. The network RBD consists of $(\sqrt{N_{min}} - 1)^2$ block-1's in series with $2(\sqrt{N_{min}} - 1)$ block-2's.

Fig3 shows the *RBD block* for a single node in the network. A node can be modeled in two ways depending on its position in the sensor field. This distinction based on its position is made due to a simple observation that nodes at the right edge of the sensor field (region-2) do not have any right neighbor (node b) as opposed to nodes in region-1. Also, nodes at the bottom edge of the sensor field (region-2) do not have a bottom neighbor (node c) as opposed to the nodes in region-1. From simple calculations we see that an N node network has $(\sqrt{N_{min}} - 1)^2$ sensor nodes in region-1 and $2(\sqrt{N_{min}} - 1)$ nodes in region-2. Hence, the network *RBD* consists of $(\sqrt{N_{min}} - 1)^2$ block-1's in series with $2(\sqrt{N_{min}} - 1)$ block-2's . Note that as every node in a square-grid, node a has four neighbors, but its relationship with only two neighbors is modeled in its *RBD block*. This is because the relationship with the other two neighbors will be modeled when their *RBD blocks* are constructed. If this is not followed then the relationship between every node-neighbor pair will be modeled twice.

If $S_a(t)$, $S_b(t)$ and $S_c(t)$ are the survival functions of nodes a, b and c respectively, then the survival function of block-1, S_{block1} is [2]:

$$s_{block1} = 1 - (1 - s_a)(1 - s_b s_c) \quad (12)$$

Since all nodes are identical, they have identical survivor functions s. Hence (12) is simplified to:

$$s_{block1} = 1 - (1 - s)(1 - s^2) = s + s^2 - s^3 \quad (13)$$

A similar analysis is carried out for nodes belonging to region-2. If s_x and s_y are the survivor functions of nodes x and y respectively, then the survivor function of block-2, s_{block2} is:

$$s_{block2} = 1 - (1 - s_x)(1 - s_y) \quad (14)$$

Since all nodes are identical, they have identical survivor functions s. Hence (14) is simplified to:

$$s_{block2} = 1 - (1 - s)(1 - s) = 2s - s^2 \quad (15)$$

Since the network *RBD* consists of $(\sqrt{N_{min}} - 1)^2$ block-1's and $2(\sqrt{N_{min}} - 1)$ block-2's in series, the network survivor function for the square grid placement scheme is:

$$s_{network} = (s_{block-1})^{(\sqrt{N_{min}}-1)^2} (s_{block-2})^{2(\sqrt{N_{min}}-1)} \quad (16)$$

The required *cdf* and *pdf* of the network lifetime can be obtained from this survival function using (9) and (7).

2) Hex-Grid: The analysis for the hex-grid is carried out on the same lines as that of the square-grid. Fig 1 shows that as in the case of a square grid, two neighboring node failures causes network failure. The RBD for this case is shown in Fig 4.

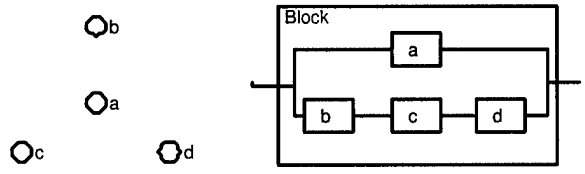


Fig. 4. RBD block for a single node in the Hex-grid: The network RBD consists of $N/2$ such blocks in series., where N is the number of nodes in the network.

[2]For notational convenience we use s_i to represent the survivor function of any node i, instead of $S_i(t)$ without any loss in generality.

If nodes a,b,c and d have identical survival functions, as in the square-grid, then the survival function of the block shown in the figure is given by:

$$s_{block} = 1 - (1 - s)(1 - s^3) \tag{17}$$

Since $N_{min}/2$ such blocks connected in series represent the network, the network survival function is given by:

$$s_{network} = (s_{block})^{N/2} \tag{18}$$

Once again after survival function of the network is obtained, the cdf and pdf are obtained from it using (9) and (7).

C. Lifetime of high density networks

The network lifetime for dense placement of sensor nodes was defined as the time to failure of $N - N_{min} + 2$ nodes, where N is the number of nodes deployed and N_{min} is the number of sensor in a minimum density deployment. This network can be modeled as a *k-out-of-n:F* system. The k out of n system is a special case of parallel redundancy. An n component system that fails if and only if at least k of the n components fail is called a k-out-of-n:F system.

Recall that in Section IV-A.2 the *cdf* of a random variable was defined as the proportion of the entire population that fails by time t. We define the network lifetime as the time to failure of $N - N_{min} + 2$ nodes. If $T_{network}$ is the lifetime of the dense network under consideration, then,

$$F(T_{network}) = \frac{N - N_{min} + 2}{N} \tag{19}$$

The network lifetime distribution of the minimum density network that employs the same pattern can be found using the analysis in Section II-D, and the lifetime of the dense network can be evaluated.

V. SIMULATION

We ran extensive simulations to:

- evaluate the *pdf*of lifetime of a single node;
- validate the theoretical analysis for the *pdf* of lifetime of a single node;
- evaluate the *pdf* of network lifetime for a square-grid;
- validate the theoretical analysis for the *pdf* of the network lifetime for a square-grid;
- evaluate the *pdf* of network lifetime for a hex-grid; and to
- validate the theoretical analysis for the *pdf* of the network lifetime for a hex-grid;

A. Node Lifetime Distribution

The first set of simulations was aimed at estimating the *pdf* of the lifetime of a node, theoretically as described in Section III and through simulations. The node, at any time can be one of its two modes of operation, *active* or *idle*. The probabilities with which a node remains in each of these modes were defined by the network protocol used. Simulation results, which are reported in Figure 5, show that the theoretical pdf matches very closely with the actual pdf.

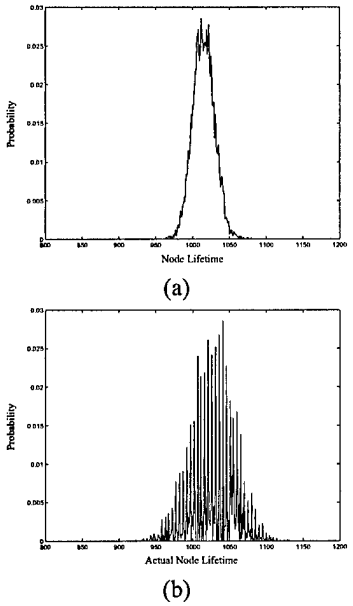


Fig. 5. Probability Density Function of the lifetime of a node. (a) Theoretical *pdf*, (b) Actual *pdf*.

B. Network Lifetime Distributions

The second set of simulations were aimed at estimating the *pdf* of the lifetime of the network, when it uses the square-grid placement and the hex-grid placement, using the theoretical analysis described in Sections IV-B.1 and IV-B.2 respectively. In both cases 36 nodes were deployed and the distance between neighboring nodes was assumed to be the same. Equations (16) for the square-grid and (18) for the hex-grid were used with $N = 36$. Figs 6(a) and (b) show the theoretical and actual *pdf* obtained for the square-grid. Figs 7(a) and (b) show the theoretical and actual pdf of a 36 node hex-grid. Figs 6 and 7 indicate that the theoretical results agree closely with the actual results[3].

Also, for networks which fail when the first node dies [2], the network lifetime analysis will be very similar to the

[3]Note that edge effects are neglected in the theoretical analysis described in Section IV.

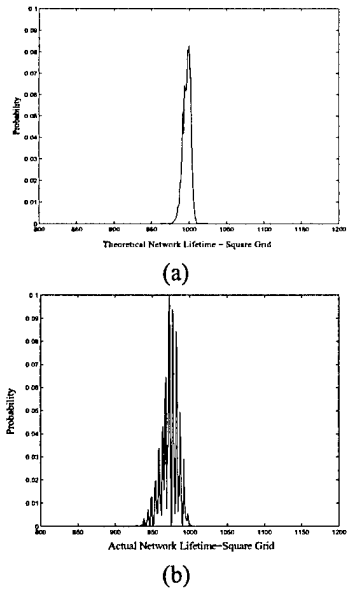


Fig. 6. Probability Density Function of the network lifetime employing the square-grid placement scheme. (a) Theoretical *pdf*, (b) Actual *pdf*.

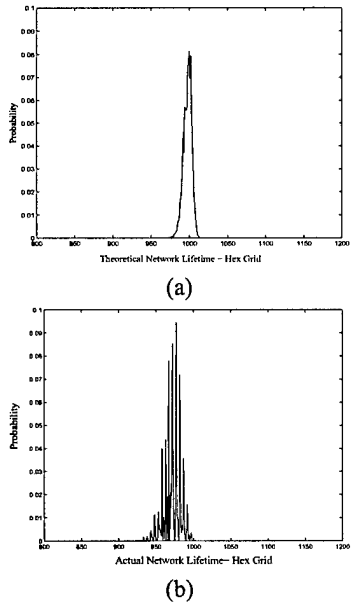


Fig. 7. Probability Density Function of the network lifetime employing the hex-grid placement scheme. (a) Theoretical *pdf*, (b) Actual *pdf*.

work in this paper. The network can then be modeled as a simple series connected block diagram, and the survival function of the network will simply be the product of the survival function of the N nodes that constitute the network.

VI. Conclusion

One of the key challenges in networks of energy constrained wireless nodes is the maximization of lifetime. If the application allows placement of sensor nodes, then our goal of maximizing the lifetime can be aided by choosing a suitable placement pattern. In this paper we evaluated the lifetime of a network employing two simple placement patterns. In evaluating the lifetime we came up not with any particular value, but a probability density function *pdf* for minimum network lifetime. We followed a *bottom-up* approach, by first evaluating the node lifetime *pdf* and then going on to finding the network lifetime *pdf*. The theoretical results as well as the methodology used will enable analysis of other sensor placement schemes, study of lifetime-cost tradeoffs, and performance analysis of energy efficiency related algorithms.

Acknowledgment

This work was supported by the Office of Naval Research (ONR) Young Investigator Award under Grant N00014-03-1-0466

References

[1] Chee-Yee Chong, S. P. Kumar, "Sensor Networks: Evolution, Opportunities, and Challenges" *Proc. IEEE* , vol 91, no. 8 , Aug 2003, pp. 1247 -1256

[2] K. Kar, S. Banerjee, "Node Placement for Connected Coverage in Sensor Networks" *Extended Abstract. Proc. WiOpt 2003, Sophia-Antipolis, France,*, March 2003.

[3] D. M. Blough, P. Santi, "Investigating Upper Bounds on Network Lifetime Extension for Cell-Based Energy Conservation Techniques in Stationary Ad Hod Networks" *Proc. MOBICOM'2002, Atlanta, Georgia,* , Sep 2002

[4] M. Bhardwaj, T. Garnett, A. Chandrakasan, "Upper Bounds on the Lifetime of Sensor Networks" *Proc. IEEE International Conference on Communications,* pp.785-790, 2001.

[5] B. Healy, "The Use of Wireless Sensor Networks for Mapping Environmental Conditions in Buildings" *ASHRAE Seminar, July 2 2003* Available Online: http://www.nist.gov/tc75/ASHRAESummer2003SeminarHealy.pdf

[6] A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, J. Anderson, "Wireless Sensor Networks for Habitat Monitoring" *Proc. WSNA'02, Atlanta, Georgia,* Sep 28, 2002.

[7] V. A. Kottapalli, A. S. Kiremidjian, J. P. Lynch, Ed Carryer, T. W. Kenny, "Two-tired wireless sensor network architecture for structural health monitoring" *Proc. SPIE, San Diego, CA,* Mar 2003.

[8] L. M. Leemis, "Reliability: Probabilistic Models and Statistical Methods," Prentice- Hall, 1995

[9] S. S. Dhillon, K. Chakrabarty, S. S. Iyengar, "Sensor Placement for Grid Coverage under Imprecise Detections," FUSION, 2002.

[10] Life Data Analysis Reference. [Online] Available: http://www.weibull.com/lifedatawebcontents.htm

Sensor Placement and Lifetime of Wireless Sensor Networks: Theory and Performance Analysis

Ekta Jain and Qilian Liang
Department of Electrical Engineering
University of Texas at Arlington
Arlington, TX 76019-0016 USA
E-mail: jain@wcn.uta.edu, liang@uta.edu

Abstract

Increasing the lifetime of energy constrained wireless sensor networks is one of the key challenges in sensor network research. In this paper, we present a *bottom-up* approach to evaluating the lifetime performance of networks employing two basic sensor placement schemes: square-grid and hex-grid. Lifetimes of individual sensor nodes as well lifetimes of networks are modeled as random variables and their probability density functions (pdf) are obtained theoretically. Reliability theory is used for the network lifetime analysis, and provides a methodology for similar studies. Simulation results show that the actual pdf's are very close to those obtained theoretically. The theoretical results provided in this paper will serve as a basis for other related research such as analysis of other sensor placement schemes, lifetime and sensor density tradeoff study, and performance of energy efficiency related algorithms.

Index Terms

Wireless Sensor Networks, sensor node placement, node lifetime, network lifetime, pdf, cdf, reliability theory, survival function.

I. Introduction

Sensor networks represent a significant advancement over traditional invasive methods of monitoring and are more economical for long term data collection and monitoring when compared

to the traditional personnel-rich methods. Although most military applications require random deployment of sensor nodes, a number of non-military applications allow the explicit placement of sensors at specific locations. Such placement-friendly sensor networks are widely used for infrastructure security, environment and habitat monitoring, traffic control etc. [1]. An in-depth study of a real-world 32 node habitat monitoring sensor network system presented in [8] is deployed on a small island off the coast of Maine to study nesting patterns of Petrels. Another such application [7] involves the use of sensors in buildings for environmental monitoring which may include chemical sensing and detection of moisture problems. Structural monitoring [9] and inventory control are some other applications of such networks.

Wireless sensor networks comprise of small, energy constrained sensor nodes. Each node basically consists of a single or multiple sensor module, a wireless transmitter-receiver module, a computational module, and a power supply module. These networks are usually employed to collect data from environments where human intervention after deployment, to recharge or replace node batteries may not be feasible, resulting in limited network lifetime. Most applications have pre-specified lifetime requirements, for instance the application in [8] has a lifetime requirement of at least 9 months. Thus estimation of lifetime of such networks prior to deployment becomes a necessity. Prior works on evaluation of lifetime have considered networks where sensor nodes are randomly deployed. [4] gives the upper bound on lifetime that any network with the specified number of randomly deployed nodes, source behavior and energy can reach while [3] discusses the upper bounds on lifetime of networks with cooperative cell based strategies.

We are concerned with networks which allow the placement of sensor nodes in specific positions. These positions depend on a number of factors which include, but are not limited to, sensing and communication capabilities of the sensor nodes, sensor field area and cost of deployment which is connected to the density of the network.

In this paper, we deal with the issues of sensor placement and lifetime estimation, and present a *bottom-up* approach to lifetime evaluation of a network. As a first step in this direction we investigate the lifetime behavior of a single sensor node and then apply this knowledge to arrive at the network lifetime behavior for two basic placement schemes. We believe that these simple schemes can serve as basis for evaluation of more complex schemes for their lifetime performance prior to deployment and help justify their deployment costs. We remark that our investigation can be applied to a network employing any routing protocol, and energy

consumption scheme. Although in a less direct way, our analysis can also be used to assess various energy efficiency related algorithms for their lifetime performance. Also, since our analysis incorporates lifetime evaluation for minimum as well as high density placement, the tradeoff between cost of deployment and lifetime can be studied because higher density implies higher cost. Our analytical results are based on the application of reliability theory. These results are supported by extensive simulations, which validate our analysis.

The rest of this paper is organized as follows. Section II details the model used for this study and provides basic discussions on coverage, connectivity and lifetime. Section III describes the lifetime analysis of a single node and Section IV uses reliability theory to apply node lifetime analysis to network lifetime analysis. Simulation and discussion of the key results of this work is presented in Section V, and Section VI concludes this paper.

II. Preliminaries

A. Basic Model

Consider identical wireless sensor nodes placed in a square sensor field of area A. All nodes are deployed with equal energy. Each sensor is capable of sensing events up to a radius r_s, the sensing range. We also define a communication range r_c, beyond which the transmitted signal is received with signal to noise ratio (SNR) below the acceptable threshold level. We assume the communication range r_c to be equal to the sensing range r_s. The communication range depends on the transmission power level, gains of the transmitting and receiving antennae, interference between neighboring nodes, path loss, shadowing, multi path effects etc. Direct communication between two sensor nodes is possible only if their distance of separation r is such that $r \leq r_c$. We call such nodes *neighbors*. Communication between a sensor node and its non-neighboring node is achieved via peer-to-peer communication. Thus the maximum allowable distance between two nodes who wish to communicate directly is $r_{max} = r_c = r_s$. A network is said to be deployed with minimum density when the distance between its neighboring nodes is $r = r_{max}$.

B. Placement Schemes

The simplest placement schemes involve regular placement of nodes such that each node in the network has the same number of neighbors. We arrive at two basic placement schemes by considering cases where each sensor nodes has four and three neighbors. This leads us to the

square-grid and *hex-grid* placement schemes shown in Fig. 1(a) and (b) respectively. A sensor node placement scheme that uses two neighbors per sensor node has been described in [2]. We believe that these three elementary placement schemes can serve as basis for other placement schemes, because a placement scheme of any complexity can be decomposed into two-neighbor, three-neighbor and four-neighbor groups. Both grids shown have the same number of nodes[1] and nodes in both grids are equidistant from their respective neighbors (with distance of separation r).

C. Coverage and Connectivity

Coverage and connectivity are two important performance metrics of networks and hence a discussion on them becomes imperative before the lifetime of the network can be defined. Coverage scales the adequacy with which the network covers the sensor field. A sensor with sensing range r_s is said to cover or sense a circular region of radius r_s around it. If every point in the sensor field is within distance r_s from at least one sensor node, then the network is said to provide complete or 100% coverage.

Various levels of coverage are acceptable depending on the application. In critical applications, complete coverage is required at all times. Any loss of coverage leads to a sensing gap in the field. Such gaps cause breach of security in case of surveillance applications. Also, in applications which require data with high precision , a sensing gap leads to inaccuracies. For such networks any loss of coverage renders the network nonfunctional. In some other applications a small loss of coverage may be acceptable.

Connectivity scales the adequacy with which nodes are able to communicate with their peers. One of the strengths of sensor networks arises from their ability to aggregate data collected from different sensor nodes. This requires adequate communication between sensor nodes. Any node should be able to communicate with any other node for proper functioning of the network. If a single node gets isolated due to failure of all its neighbors, it will be unable to communicate with the rest of the network. If a large number of nodes fail due to lack of energy, a part of the network may get completely disconnected from the rest. In our analysis we assume that only 100% connectivity is acceptable and the network fails with any loss of connectivity.

[1]The *Hex-grid* has lower density than the *Square-grid*. With 36 nodes deployed, the network with *Square-grid* covers an area of $25r^2$, and the *Hex-grid* covers an area of $48r^2$, almost double that of the *square grid*.

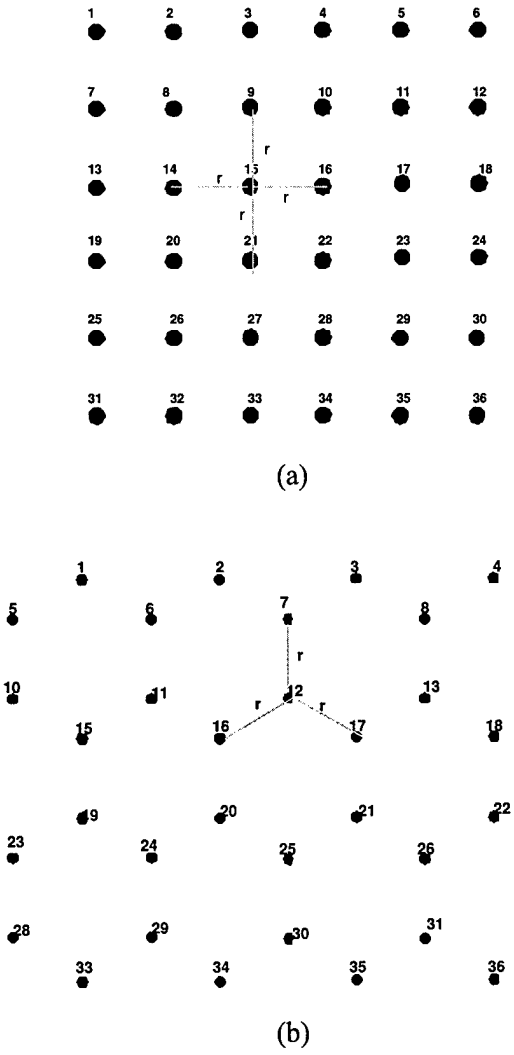


Fig. 1. Placement Schemes for a 36 node sensor network: (a) Square-Grid (b) Hex-Grid.

An example of a sensor placement scheme that concentrates mainly on coverage as its parameter of interest can be found in [11], where a sensor placement algorithm for grid coverage has been proposed. In our analysis we require the network to provide complete coverage and connectivity. We give equal importance to both parameters and declare the network nonfunctional if either of them falls below their desired levels.

D. Lifetime

The basic definition of lifetime, or more precisely the post-deployment active lifetime of a network is the time measured from deployment until network failure. Based on the levels of coverage and connectivity required to deem a network functional, network failure can be interpreted in different ways. Since only complete coverage and connectivity are acceptable to us, network failure corresponds to the first loss of coverage or connectivity.

In this paper, we concentrate on finding the minimum lifetime of a network, the worst case scenario. To be able to evaluate this minimum lifetime, we need to know the lifetime of a single sensor node the, the minimum number of node failures that cause network failure, and the positional relationship [2] between the failed nodes.

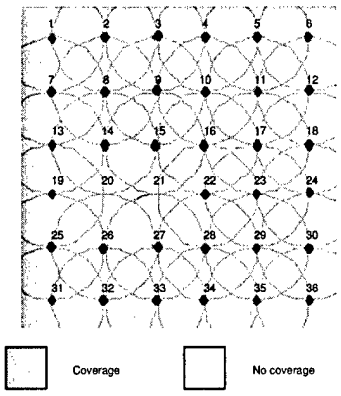
1) Minimum Density Networks: Consider the square-grid and the hex-grid deployed with minimum density. Both schemes survive the failure of a single node without loss of either connectivity or coverage implying that the minimum number of node failures that can lead to network failure is greater than one. Failure of any two neighboring nodes causes loss of coverage and hence network failure as indicated in Figs 2(a) and (b).

Thus the minimum number of node failures that cause network failure is two and these two nodes must be adjacent to each other (neighbors). A network may undergo multiple node failures and still be connected and covered if any of the failed nodes are not neighbors. But the absolute minimum number of node failures that can cause network failure is two.

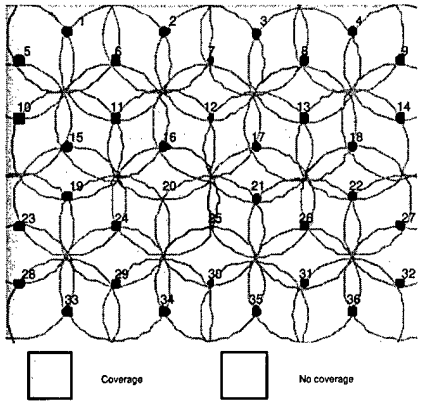
2) Network lifetime for dense placement: Let N_{min} be the number of sensor nodes deployed in a sensor field of area A with minimum density. In a minimum density network, the separation between neighbors is r_{max}, the maximum range of the sensor nodes. A network deployed with higher density would require a larger number of nodes N, $N > N_{min}$ and smaller separation between neighboring nodes r, $r < r_{max}$. Since the range of a sensor node r_{max} is greater than the distance to its immediately adjacent nodes, it is now be able to communicate not only with the nodes immediately adjacent to it, but also with other nodes which fall in its range. In other words, each node now has more number of neighbors that any node in a minimum density network.

We discussed earlier that the minimum lifetime of a square-grid or hex-grid network with

[2]Positional relationship between two nodes can be that the two nodes are diagonal, adjacent or completely unrelated.



(a)



(b)

Fig. 2. Loss of coverage due to failure of two neighboring nodes: (a)Square-grid: Failure of nodes 20 and 21 causes loss of coverage. (b)Hex-grid: Failure of nodes 20 and 25 causes loss of coverage.

$r = r_{max}$(minimum density) is the time to failure of two neighboring nodes. High density networks can lose $(N - N_{min})$ nodes and still be deployed with minimum density and fail only after the further loss of a minimum of two neighboring nodes. Since the network after $(N - N_{min})$ node failures is deployed with minimum density, the time taken for the failure of any two neighboring nodes would be equal to the minimum lifetime of a minimum density network (T_{md}) which was discussed in the preceding section. If t_{dense}, the time taken for the failure of $(N - N_{min})$ nodes can be found, we define the lifetime of a high density network

(T_{hd}) as:

$$T_{\text{hd}} = t_{\text{dense}} + T_{\text{md}} \tag{1}$$

III. Node Lifetime Evaluation

We begin our analysis with the estimation of the lifetime of a single sensor node. A node is said to have m possible modes of operation, and at any given time the node is in one of these m modes. Let w_i be the fraction of time that a node spends in the i^{th} mode, where w_i's are such that,

$$\sum_i w_i = 1 \;\; i = 1, 2...m \tag{2}$$

The w_i's do not remain constant in general and vary for different networks scenario's. Hence they are modeled as random variables that take values from 0 to 1 according to specific probability distribution functions (*pdf*)'s which we attempt to find.

We assume that the total node energy at the time of deployment is E_{total} and that the node spends a power of P_i watts/unit time, while in the i^{th} mode. If T_{node} is the lifetime of the node, then the node spends $w_i T_{node}$ time units in mode i. We define the lifetime of a node as the time from deployment to when its energy drops below a threshold energy value E_{th}. The following equation follows from this definition and from the fact that E_{th} is negligible compared to E_{total}.

$$\begin{aligned} E_{total} - \sum_i w_i P_i T_{node} &\geq E_{th} \\ T_{node} &\geq \frac{E_{total}}{\sum_i w_i P_i} \end{aligned} \tag{3}$$

We observe from this equation that T_{node} is a function of the random variables w_i and hence is a random variable itself. This is an important observation as it implies that since the modes of the various nodes cannot be known *a priori*, the lifetime of a single node can be best represented as a random variable that takes different values with certain probabilities defined by its probability density function (*pdf*) $f_t(t)$. In order to obtain the *pdf* of T_{node}, we first find the *pdf* of $w_i \forall i$.

To this purpose we assume that at any given time a node can be in one of its two modes of operation, *active* or *idle*. A node is *active* when it is either transmitting or receiving and is *idle* otherwise. If p is the probability of node being active, $1-p$ is the probability of the node being idle at any given time.

$$Pr\{\text{node is active}\} = p \tag{4}$$

$$Pr\{\text{node is idle}\} = 1 - p \tag{5}$$

Note that the actual values of p will depend on the energy efficiency related algorithms used such as energy efficient routing protocols and energy consumption schemes. Let w_1 and w_2 be the fraction of time the node is in active and idle mode respectively. Since we assume only two modes of operation, $w_2 = 1 - w_1$. The random variable w_1 is clearly binomial in nature, with probability of success, i.e., probability of node in active mode being p. We observe the node over T time units. Since w_1 has a binomial distribution, the probability of the node being active for x time units of a total of T time units is give by,

$$P\{w_1 = x\} = C_T^x p^x (1-p)^{T-x} \tag{6}$$

As T becomes large, the binomial distribution can be approximated to a normal distribution with mean $\mu = Tp$ and variance $\sigma^2 = np(1-p)$. Since $w_2 = 1 - w_1$, w_2 also follows normal distribution with mean $\mu = T(1-p)$ and variance $\sigma^2 = np(1-p)$. Hence we conclude that the fraction of time that the node spends in any mode follows the normal distribution.

We observe from equation (3) that the denominator of the expression is a normal random variable because it is the sum of m normal random variables. This helps us draw an important conclusion that the reciprocal of the lifetime of a node follows the normal distribution.

IV. Network Lifetime Analysis using Reliability Theory

Since the lifetimes of an individual node is not constant but a random variables, it follows that the network lifetime is also a random variable. We apply reliability theory to find the distribution of the network lifetime, given the node lifetime distribution. The following section treats the basics of reliability theory before going on to its application.

A. Reliability Theory

Reliability theory is concerned with the duration of the useful life of components and systems of components [12] [10] [5]. We model the lifetime (of individual nodes and the network) as a continuous non-negative random variable T. Below, we describe three of the many ways of defining this non-negative random variable T.

1) Probability Density Function (pdf): The *pdf* gives the probability of the random variable taking a certain value [6]. It is represented as $f(t)$ and has a probabilistic interpretation

$$f(t)\Delta t = P\left[t \leq T \leq t + \Delta t\right] \tag{7}$$

for small values of Δt. All *pdf*'s must satisfy two conditions, $\int_0^\infty f(t)dt = 1$ and $f(t) \geq 0, \forall t$.

The lifetime of any item can be thought of as the time until which the item survives, or the time at which the item fails, i.e., time to failure. The *pdf* represents the relative frequency of failure times as a function of time.

We have the distribution of the lifetime of a node in the form of its *pdf*, in that we know that the reciprocal of the node lifetime has a normal *pdf*.

2) Cumulative Distribution Function (cdf): The *cdf* corresponding to the *pdf* $f(t)$ is denoted by $F(t)$ and is very useful as it gives the probability that a randomly selected component or system will fail by time t. It can be expressed in three different ways:

- $F(t)$ = the area under the *pdf* $f(t)$ to the left of t.
- $F(t)$= the probability that a single randomly chosen new component will fail by time t.
- $F(t)$= the proportion of the entire population that fails by time t.

The relationship between the *cdf* and *pdf* of a random variable is given below:

$$F(t) = \int_0^t f(s)ds \tag{8}$$

The *pdf* and the *cdf* are the two most important statistical functions in reliability theory. They are closely related as shown by equation(8). They give a complete description of the probability distribution of the random variable. The knowledge of these two functions enables us to find any other reliability measure.

From the relationship between the *cdf* and the *pdf* defined in equation (8), and the interpretation of the *pdf* as the relative frequency of failure times, we interpret the *cdf* of the lifetime T as the probability that the item in question will fail before the associated time value, t. As a result the *cdf* is sometimes called the *unreliability* function.

3) Survivor Function: The *Survivor function* $S(t)$, also known as the *Reliability function* $R(t)$ can be derived using the interpretation of the *cdf* as the unreliability function. It is defined as the probability that a unit is functioning at any time t:

$$S(t) = P\left[T \geq t\right] \quad t \geq 0 \tag{9}$$

Since a unit either fails, or survives, and one of these two mutually exclusive alternatives must occur, we have,

$$S(t) = 1 - F(t) = 1 - \int_0^t f(s)ds \tag{10}$$

All survivor functions must satisfy three conditions: $S(0) = 1$, $\lim_{t\to\infty} S(t) = 0$, and $S(t)$ is non increasing.

There are two interpretations of the survival function. First, $S(t)$ is the probability that an individual item is functioning as time t. This interpretation will be used later in finding the lifetime distribution of the network from the lifetime distribution of its constituent nodes. Second, if there is a large population of items with identical distributed lifetimes, $S(t)$ is the expected fraction of the population that is functioning at time t. This interpretation will be used in finding the time taken for $(N - Nmin)$ node failures for estimation of the minimum lifetime of dense networks.

We obtain the *pdf* of the lifetime of a single sensor node from Section III. Using equations (8) and (10) we obtain the survivor function $S(t)$ of a single sensor node. Note that all sensor nodes are assumed to be identical with survivor functions $S(t)$.

4) System Reliability: A system is a collection of components arranged in a specific The main objective of system reliability is the construction of a distribution that represents the lifetime of a system based on the lifetime distributions of the components from which it is composed. To accomplish this, we consider the relationship between components. This approach to finding system lifetime has the inherent advantage that it is often easier and cost-effective to extensively test a single component or subsystem rather the whole system.

5) Reliability Block Diagram: Reliability block diagram (*RBD*) is a graphical representation of the components of the system, and provides a visual representation of the way components are reliability-wise connected. Thus the effect of the success or failure of a component on the system performance can be evaluated.

Consider a system with two components. If this system is such that a single component failure can render the system nonfunctional, then we say that the components are reliability-wise, connected in series. If the system fails only when both its components fail, then we say that the components are reliability-wise connected in parallel. Note that the physical connection between the component may or may not be different from their reliability-wise connection. The

RBD's for both cases are given in Figs.3.If $S_1(t)$ and $S_2(t)$ are the survival functions of the two components, the system survival functions $S(t)_{series}$ and $S(t)_{parallel}$, for the series and parallel cases are given in equations (11) and (12) respectively.

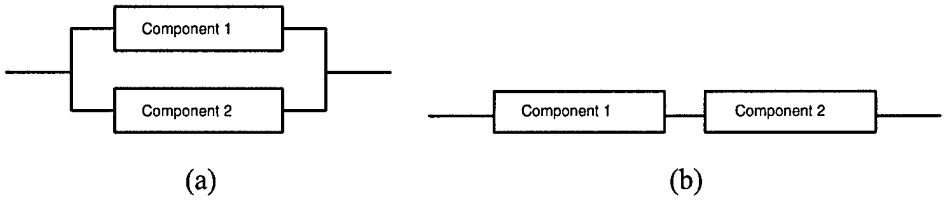


Fig. 3. Reliability block diagrams (*RBD*) for a system of two components. (a)RBD with series connected components. (b)RBD with parallel connected components.

$$S_{series}(t) = S_1(t)S_2(t) \tag{11}$$

$$S_{parallel}(t) = 1 - [(1 - S_1(t))(1 - S_2(t))] \tag{12}$$

Any complex system can be realized in the form of a combination of blocks connected in series and parallel, and the system survival function can be obtained by using equations (11) and (12). In our analysis, the network is the system under consideration and the sensor nodes are the components of the system. All sensor nodes are assumed to have identical survival functions $S(t)$ and their failures are supposed to be independent on one another.

B. Lifetime of Minimum Density Networks

1) Square Grid: As defined in Section II-D.1, the minimum network lifetime is the time to failure of any two neighboring nodes. We know that the failure of any single node does not cause network failure. The failure of any node coupled with the failure of any of its neighbors causes network failure. Using this definition we build the RBD for the square-grid as shown in Fig 4.

Fig4 shows the *RBD block* for a single node in the network. A node can be modeled in two ways depending on its position in the sensor field. This distinction based on its position is made due to a simple observation that nodes at the right edge of the sensor field (region-2) do not have any right neighbor (node b) as opposed to nodes in region-1. Also, nodes at the bottom

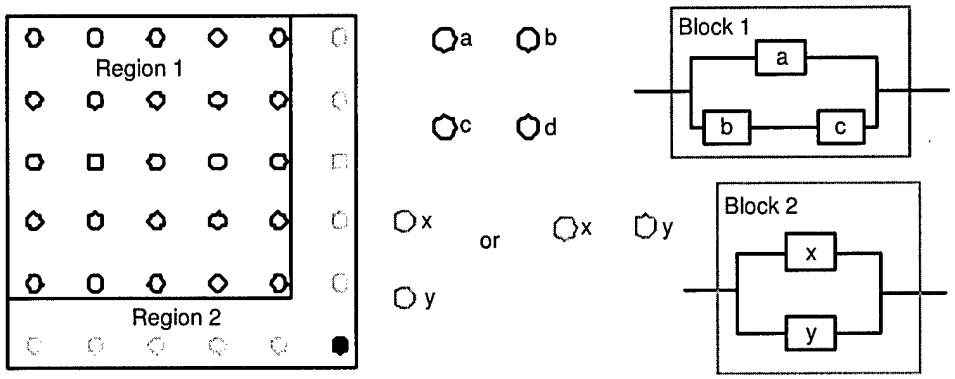


Fig. 4. RBD of a single node in a square grid. Nodes belonging to region-1 are modeled as block-1 and nodes belonging to region-2 are modeled as block-2. The network RBD consists of $(\sqrt{N_{min}}-1)^2$ block-1's in series with $2(\sqrt{N_{min}}-1)$ block-2's

edge of the sensor field (region-2) do not have a bottom neighbor (node c) as opposed to the nodes in region-1. From simple calculations we see that an N node network has $(\sqrt{N_{min}}-1)^2$ sensor nodes in region-1 and $2(\sqrt{N_{min}}-1)$ nodes in region-2. Hence, the network *RBD* consists of $(\sqrt{N_{min}}-1)^2$ block-1's in series with $2(\sqrt{N_{min}}-1)$ block-2's . Note that as every node in a square-grid, node a has four neighbors, but its relationship with only two neighbors is modeled in its *RBD block*. This is because the relationship with the other two neighbors will be modeled when their *RBD blocks* are constructed. If this is not followed then the relationship between every node-neighbor pair will be modeled twice.

If $S_a(t)$, $S_b(t)$ and $S_c(t)$ are the survival functions of nodes a, b and c respectively, then the survival function of block-1, S_{block1} is [3]:

$$s_{block1} = 1-(1-s_a)(1-s_b s_c) \tag{13}$$

Since all nodes are identical, they have identical survivor functions s. Hence (13) is simplified to:

[3]For notational convenience we use s_i to represent the survivor function of any node i, instead of $S_i(t)$ without any loss in generality.

$$\begin{aligned} s_{block1} &= 1-(1-s)(1-s^2) \\ &= s+s^2-s^3 \end{aligned} \tag{14}$$

A similar analysis is carried out for nodes belonging to region-2. If s_x and s_y are the survivor functions of nodes x and y respectively, then the survivor function of block-2, s_{block2} is:

$$s_{block2} = 1-(1-s_x)(1-s_y) \tag{15}$$

Since all nodes are identical, they have identical survivor functions s. Hence (15) is simplified to:

$$\begin{aligned} s_{block2} &= 1-(1-s)(1-s) \\ &= 2s-s^2 \end{aligned} \tag{16}$$

Since the network *RBD* consists of $(\sqrt{N_{min}}-1)^2$ block-1's and $2(\sqrt{N_{min}}-1)$ block-2's in series, the network survivor function for the square grid placement scheme is:

$$s_{network} = \left(s_{block-1}\right)^{(\sqrt{N_{min}}-1)^2}\left(s_{block-2}\right)^{2(\sqrt{N_{min}}-1)} \tag{17}$$

The required *cdf* and *pdf* of the network lifetime can be obtained from this survival function using (10) and (8).

2) Hex-Grid: The analysis for the hex-grid is carried out on the same lines as that of the square-grid. Fig 2 (b) shows that as in the case of a square grid, two neighboring node failures cause network failure. The RBD block of a single node is shown in Fig. 5.

Since the relation between a node and all of its neighbors is modeled by its corresponding *RBD block*, the *RBD block*'s for the neighbors is not constructed as this causes the relationship between the nodes to be considered twice. Hence the network *RBD* consists on only $N_{min}/2$ *RBD blocks* in series. If nodes a,b,c and d have identical survival functions, as in the square-grid, then the survival function of the block shown in the figure is given by:

$$s_{block} = 1-(1-s)(1-s^3) \tag{18}$$

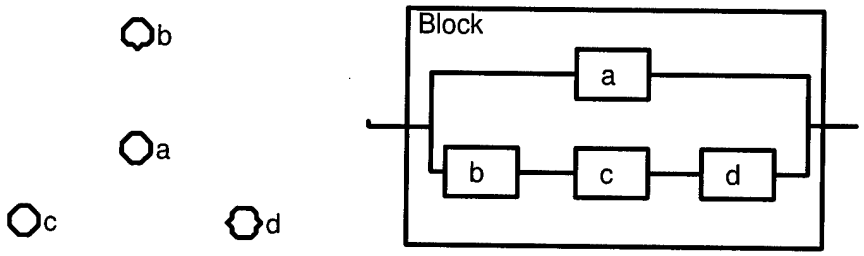


Fig. 5. RBD block for a single node in the Hex-grid: The network RBD consists of $N/2$ such blocks in series.

Since $N_{min}/2$ such blocks connected in series represent the network, the network survival function is given by:

$$s_{network} = (s_{block})^{N/2} \tag{19}$$

Once again after survival function of the network is obtained, the cdf and pdf are obtained from it using (10) and (8).

C. *Lifetime of High Density Networks*

The network lifetime for dense placement of sensor nodes is given by equation (1) and was defined in Section II-D.2 as the time to failure of any two neighboring nodes after $(N - N_{min})$ nodes have failed, where N is the number of nodes deployed and N_{min} is the number of sensor in a minimum density deployment. We now concentrate on finding the time taken for $N - N_{min}$ node failure, t_{dense}. This situation can be modeled as a *k-out-of-n:F* system. The k out of n system is a special case of parallel redundancy. An n component system that fails if and only if at least k of the n components fail is called a k-out-of-n:F system.

Recall that in Section IV-A.3 the survivor function $S(t)$ of an item was interpreted as the expected fraction of the population that functions at time t. Since t_{dense} is the time taken for $N - N_{min}$ node failures, the fraction of nodes that are functioning at time t_{dense} is N_{min}/N. The time t_{dense} is such that:

$$S\left(t_{dense}\right) = \frac{N_{min}}{N} \tag{20}$$

,where S(t) was defined as the survivor function of any sensor node in Section IV-A.3. Since S(t) can be found with the knowledge of the *pdf* of the node lifetime, t_{dense} can be evaluated from equation (20) and the minimum lifetime of a high density network can be evaluated using (1)

V. SIMULATION

We ran extensive simulations to:

- evaluate the *pdf*of lifetime of a single node;
- validate the theoretical analysis for the *pdf* of lifetime of a single node;
- evaluate the *pdf* of network lifetime for a square-grid;
- validate the theoretical analysis for the *pdf* of the network lifetime for a square-grid;
- evaluate the *pdf* of network lifetime for a hex-grid; and to
- validate the theoretical analysis for the *pdf* of the network lifetime for a hex-grid;

A. Node Lifetime Distribution

The first set of simulations was aimed at estimating the *pdf* of the lifetime of a node, theoretically as described in Section III and through simulations. The node, at any time can be one of its two modes of operation, *active* or *idle*. The probabilities with which a node remains in each of these modes were defined by the network protocol used. Simulation results, which are reported in Figure 6, show that the theoretical pdf matches very closely with the actual pdf.

B. Network Lifetime Distributions

The second set of simulations were aimed at estimating the *pdf* of the lifetime of the network, when it uses the square-grid placement and the hex-grid placement, using the theoretical analysis described in Sections IV-B.1 and IV-B.2 respectively. In both cases 36 nodes were deployed and the distance between neighboring nodes was assumed to be the same. Equations (17) for the square-grid and (19) for the hex-grid were used with $N = 36$. Figs 7(a) and (b) show the theoretical and actual *pdf* obtained for the square-grid. Figs 8(a) and (b) show the theoretical and actual pdf of a 36 node hex-grid. Figs 7 and 8 indicate that the theoretical results agree closely with the actual results[4].

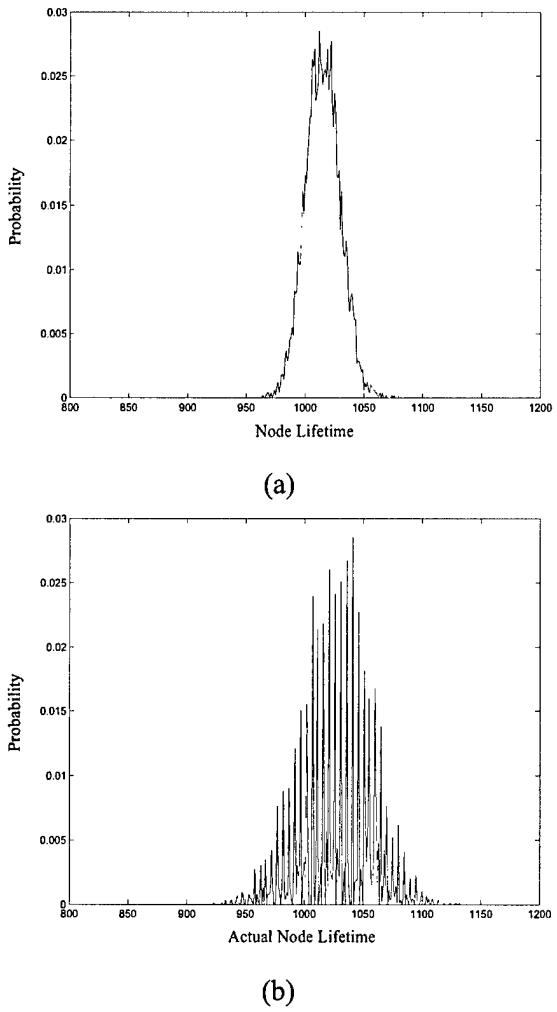


Fig. 6. Probability Density Function of the lifetime of a node. (a) Theoretical *pdf*, (b) Actual *pdf*.

Also, for networks which fail when the first node dies [2], the network lifetime analysis will be very similar to the work in this paper. The network can then be modeled as a simple series connected block diagram, and the survival function of the network will simply be the product of the survival function of the N nodes that constitute the network.

[4]Note that edge effects are neglected in the theoretical analysis described in Section IV.

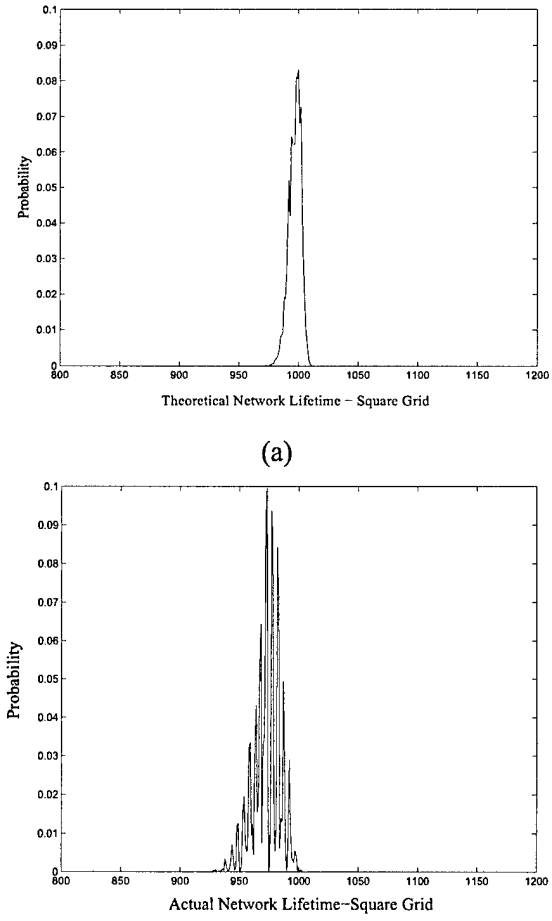


Fig. 7. Probability Density Function of the network lifetime employing the square-grid placement scheme. (a) Theoretical *pdf*, (b) Actual *pdf*.

VI. CONCLUSION

One of the key challenges in networks of energy constrained wireless nodes is maximization of the network lifetime. If the application allows placement of sensor nodes, our goal of maximizing the lifetime can be aided by choosing a suitable placement pattern. In this paper we evaluated the lifetime of a network employing two simple placement patterns. In evaluating the lifetime we came up not with any particular value, but a probability density function *pdf* for minimum network lifetime. We followed a *bottom-up* approach, by first evaluating the node lifetime *pdf* and

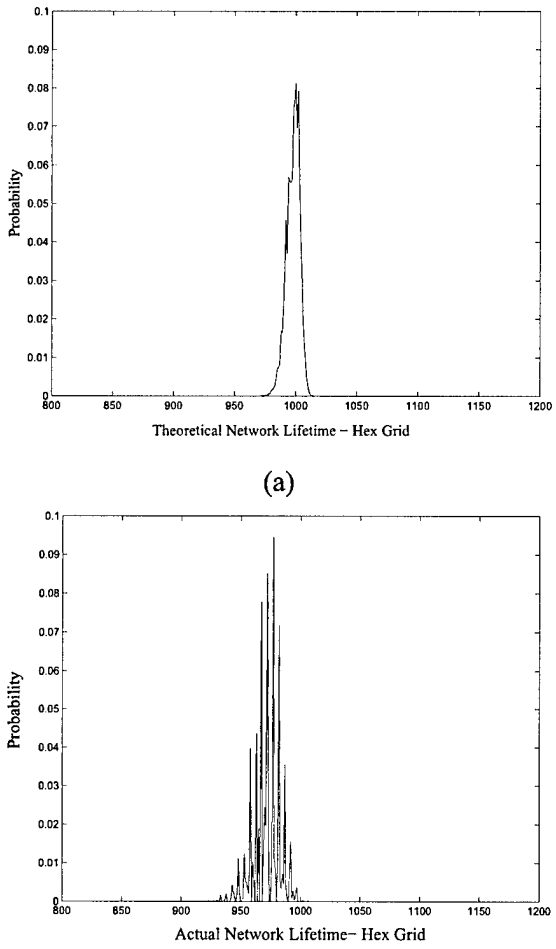


Fig. 8. Probability Density Function of the network lifetime employing the hex-grid placement scheme. (a) Theoretical *pdf*, (b) Actual *pdf*.

then going on to finding the network lifetime *pdf*. Theoretical results as well as our methodology will enable analysis of other sensor placement schemes, study of lifetime-cost tradeoffs, and performance analysis of energy efficiency related algorithms.

ACKNOWLEDGMENT

This work was supported by the US Office of Naval Research (ONR) Young Investigator Award under Grant N00014-03-1-0466

REFERENCES

[1] Chee-Yee Chong, S. P. Kumar, "Sensor Networks: Evolution, Opportunities, and Challenges" *Proc. IEEE* , vol 91, no. 8 , Aug 2003, pp. 1247 -1256

[2] K. Kar, S. Banerjee, "Node Placement for Connected Coverage in Sensor Networks" *Extended Abstract. Proc. WiOpt 2003, Sophia-Antipolis, France,*, March 2003.

[3] D. M. Blough, P. Santi, "Investigating Upper Bounds on Network Lifetime Extension for Cell-Based Energy Conservation Techniques in Stationary Ad Hod Networks" *Proc. MOBICOM'2002, Atlanta, Georgia,* , Sep 2002

[4] M. Bhardwaj, T. Garnett, A. Chandrakasan, "Upper Bounds on the Lifetime of Sensor Networks" *Proc. IEEE International Conference on Communications,* pp.785-790, 2001.

[5] D. Kececioglu, "Reliability Engineering Handbook" *Volume 1 and 2,* Prentice Hall, Ney Jersey 1991.

[6] A. Papoulis, S. U. Pillai "Probability, Random Varibales and Stochastic Processes, " *4th ed,* McGraw-Hill, New York 2002.

[7] B. Healy, "The Use of Wireless Sensor Networks for Mapping Environmental Conditions in Buildings" *ASHRAE Seminar, July 2 2003* Available Online: http://www.nist.gov/tc75/ASHRAESummer2003SeminarHealy.pdf

[8] A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, J. Anderson, "Wireless Sensor Networks for Habitat Monitoring" *Proc. WSNA'02, Atlanta, Georgia,* Sep 28, 2002.

[9] V. A. Kottapalli, A. S. Kiremidjian, J. P. Lynch, Ed Carryer, T. W. Kenny, "Two-tired wireless sensor network architecture for structural health monitoring" *Proc. SPIE, San Diego, CA,* Mar 2003.

[10] L. M. Leemis, "Reliability: Probabilistic Models and Statistical Methods," Prentice- Hall, 1995

[11] S. S. Dhillon, K. Chakrabarty, S. S. Iyengar, "Sensor Placement for Grid Coverage under Imprecise Detections," FUSION, 2002.

[12] Life Data Analysis Reference. [Online] Available: http://www.weibull.com/lifedatawebcontents.htm

An Energy-Efficient Protocol For Wireless Sensor Networks

Hsiao-Lan Hsu
Department of Electrical Engineering
University of Texas at Arlington
Arlington, TX 76019-0016
Email: hxh1670@omega.uta.edu

Qilian Liang
Department of Electrical Engineering
University of Texas at Arlington
Arlington, TX 76019-0016
Email: liang@uta.edu

Abstract— **In the paper, we consider a network of energy-constrained sensors deployed over a region. Each sensor node in such a network is systematically gathering and transmission sensed data to a base station (via clusterhead) for further processing. A key challenge in data gathering is to maximize the system lifetime, given the energy constraints. We focus on reducing the power consumption of wireless sensor networks. The dominate component in energy consumption is almost always due to communication. Therefore, we heavily modify an existing communication protocol, Low-Energy Adaptive Clustering Hierarchy (LEACH). We extend LEACH's stochastic cluster-head selection algorithm by a deterministic component to reduce energy consumption. Simulation results show that our modified scheme can extend the network life around 50% for First Node Dies (FND) and 62% for Last Nodes Dies (LND).**

Index Terms–Wireless sensor networks, energy efficiency, cluster-head selection, LEACH

I. Introduction

Wireless sensor network consists of hundreds to several thousands of small sensor nodes scattered throughout an area of interest. Sensor nodes may spontaneously create impromptu network, assemble the network themselves, dynamically adapt to device failure and degradation, manage movement of sensor nodes, and react to changes in task and network requirements. Each individual sensor contains both processing and communication elements and is designed to monitor the environment for events specified by the deployer of the network. Information about the environment is gathered by the sensors and is delivered to a central base station where the user can extract the desired data. Therefore, wireless sensor networks must be rapidly deployable, possibly multi-hop, self-organizing, and capable of multimedia service support. With these advantages in mind, these types of networks are useful in any situation where temporary network connectivity is needed, such as disaster relief, search and rescue, collaborative computing, multimedia classroom, law enforcement, distance learning and other special-purpose applications.

While their potential benefits are clear, a number of open problems must be solved in order for wireless sensor networks to become viable in practice. These problems include issues related to deployment, network lifetime, communication bandwidth, scalability, and power management. Of these, energy efficiency for extending network lifetime is one of the most important topics. Sensor nodes are likely to be battery powered, and it is often very difficult to change or recharge batteries for these nodes. Prolonging network lifetime for these nodes is a critical issue. Therefore, all aspects of the node, from hardware to the protocols, must be designed to be extremely energy efficient.

Wireless sensor networking is a broad research area, and many researchers have done research work in the new area of low power to extend network lifetime. Generally, wireless sensor networks are organized in an ad hoc fashion. For energy efficient ad hoc networks, Rodoplu and Meng [6] developed a general mathematical theory for designing a minimum power topology within one cluster for a stationary network. Their approach only considers the immediate locality of a node, and assumes that clusters have been organized and the mobile devices have similar antenna heights. Block and Baum [2] proposed an energy-efficient routing protocol for wireless sensor networks with battery level uncertainty. A new topology management scheme, called STEM (Sparse Topology and Energy Management) was proposed in [8] for sensor networks, which can wake up nodes from a deep sleep state without the need for an ultra low-power radio.

In this paper, we develop an energy efficient protocol for wireless sensor networks by heavily modifying the existing low-energy adaptive clustering hierarchy (LEACH) [3], an application-specific protocol architecture. LEACH combines the ideas of energy-efficient cluster-based routing and media access together with application-specific data aggregation to achieve good performance in terms of system lifetime, latency, and application-perceived quality. LEACH includes a new, distributed cluster formation technique that enables self-organization of large numbers of nodes, algorithms for adapting clusters and rotating cluster head positions to evenly distribute the energy load among all the nodes, and techniques to enable distributed signal processing to save communication resources. However, in LEACH, selection of cluster-heads is completely is stochastic! Each node has the same probability to become cluster-head in each round even though the battery capacities in some nodes are very low. Therefore, we developed a protocol based on LEACH to extend network lifetime and reduce the power consumption by modifying cluster-head selection algorithm.

The remainder of this paper is organized as follows. In sec-

tion II, we briefly overview the operation of LEACH protocol. In section III, we discuss the problem of selecting cluster heads in LEACH and our newly proposed protocol is presented. Section IV demonstrates the advantage of our protocol through analysis and simulation results and conclusions are drawn in Section V.

II. Overview of LEACH (Low-Energy Adaptive Clustering Hierarchy)

The purpose of LEACH is to randomly select sensor nodes as cluster-heads, so the high-energy dissipation in communicating with the base station is spread to all the sensor nodes in the sensor network. The operation of LEACH is broken up into rounds, where each round begins with a set-up phase, when the clusters are organized, followed by a steady-state phase, where several frames of data are transferred from the nodes to their cluster-head in each cluster and on to the base station, as shown in Figure 1. The nodes must all be time-synchronizes in order to start the set-up phase at the same time. In order to minimize overhead, the steady-state phase is long compared to the set-up phase.

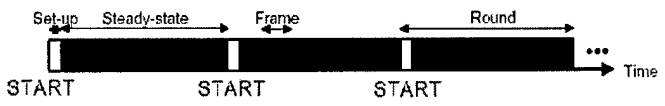


Fig. 1. Time-line showing LEACH operation

A. Set-up Phase

In the set-up phase, when clusters are being created, each node decides whether or not to become a cluster-head for the current round. This decision is based on the suggested percentage of cluster heads for the network and the number of times the node has been a cluster-head so far. Once each node that has elected itself a cluster-head for the current round broadcasts an advertisement message to the rest of the nodes. Then, each non-cluster-head node decides the cluster to which it will belong for this round. This decision is based on the received signal strength of the advertisement from each cluster head. After each node has decided to which cluster it belongs, it must inform the cluster-head node that it will be a member of the cluster.

The cluster-head node receives all the messages for nodes that would like to be included in the cluster. Based on the number of nodes in the cluster, the cluster-head node sets up a TDMA schedule telling each node about the time slot it should transmit in. This schedule is broadcast back to the nodes in the cluster. This ensures that there are no collisions among data messages and also allows the radio components of each non-cluster-head node to be turned off at all time, except during their transmit time, thus minimizing the energy dissipated by the individual sensors. After all nodes in the cluster know the TDMA schedule, the set-up phase is complete and the steady-state operation (data transmission) can begin.

B. Steady-State Phase

In the steady-state phase the nodes transmit to the cluster head when their slot in the TDMA schedule arrives. The nodes can turn themselves off and sleep while waiting for their slot. This is one of the major energy-saving features of LEACH. Once the clusters are created and the TDMA schedule is fixed, data transmission can begin. Assuming nodes always have data to send, the steady-state operation is broken into frames, where nodes send their data to the cluster head at most one per frame during their allocated transmission slot. The duration of each slot in which a node transmits data is constant, so the time to send a frame depends on the number of nodes in the cluster.

After a certain time frame the cluster set-up is repeated with new nodes becoming cluster-heads in a random manner. This randomization helps in keeping the energy dissipation in the system low and also uniformly degrades the energy for all nodes.

III. LEACH with Modified Cluster-Head Selection

A. Problem Formulation

Since data transfers to the base station dissipate too much energy, LEACH tries to evenly distribute the energy load among all nodes in the network by the cluster-head selection algorithm as described in the previous section. This rotation of cluster-heads leads to a balanced power consumption of all nodes and hence to a longer lifetime of the wireless microsensor network.

However, looking at a single round of LEACH, it is obvious that a stochastic cluster-head selection will not automatically lead to minimum energy consumption during data transfer for a given set of nodes. A cluster-head can be located near the edges of the network or adjacent nodes can become cluster heads. In these cases some nodes have to bridge long distances to reach a cluster-head as shown in Figure 2. This leads to high-energy consumption since nodes have to transmit over long distance.

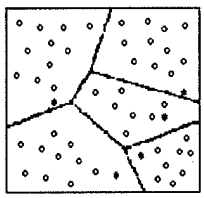


Fig. 2. The bad-case-scenario of LEACH. The cluser-head nodes are marked with solid dot

B. Solution: Uniformly Distributing Cluster-Heads

While there are advantages for using LEACH's distributed cluster formation algorithm, this protocol offers no guarantee about the placement of cluster-head nodes. Therefore, we would like the cluster-head nodes to be spread thought the network, as this will minimize the distance that the non-cluster-head nodes need to send their data. This paper

proposes a modification of LEACH's cluster head selection algorithm,which can produce better clusters to reduce energy consumption. We choose the nodes that are closest to several specific positions as cluster-heads at the beginning of each round. These positions are uniformly distributed in the network avoiding all cluster-heads can be located near the edges of the network or adjacent nodes can become cluster heads.

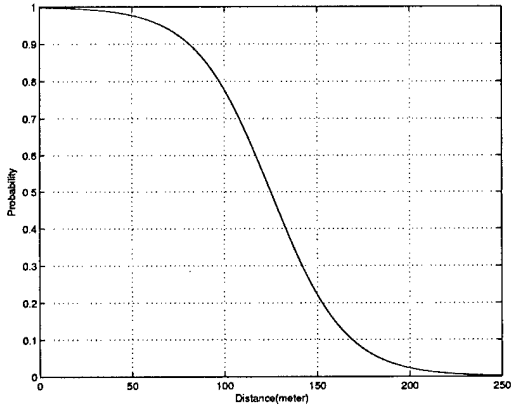


Fig. 3. The relationship between the possibility to be elected and the distance $D_i(t)$

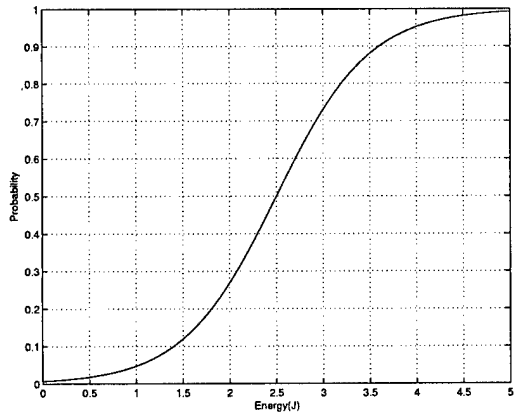


Fig. 4. The relationship between the possibility to be elected and the remaining energy $E_i(t)$

Once the clusters are formed, each non-cluster node transmit sensor data to its cluster-head in a schedule time slot and the cluster-heads transmit the aggregated data to the base station as described in LEACH. After transmission in each frame, the node with highest energy capacity in each cluster to be the cluster-head of next frame. This can be achieved by setting the probability of becoming a cluster head as a function of a node's energy level relative to the aggregate energy remaining in the network, rather than purely as a function of the number of times the node has been cluster head. Thus, if there are nodes in the network, each node should choose to become a cluster head with probability

$$P_i(t) = \frac{E_i(t)}{E_{total}(t)} \tag{1}$$

where $E_i(t)$ is the current energy of node i and

$$E_{total}(t) = \sum_{i=1}^{N} E_i(t) \tag{2}$$

Using these probabilities, the nodes with higher energy level are more likely to become cluster heads than nodes with less energy level.

C. A further modification of LEACH

In LEACH, when the sensor nodes have varied energy capacities in practice, central control was applied (e.g., assuming the total amount of energy of the sensor network was known). Besides the existing energy level of each node, we believe the physical location of each node should also be taken into consideration. In this paper, we use a sigmoid function to denote the possibility to be elected as a cluster head (versus distance),

$$g(D_i(t)) = \frac{1}{1 + e^{-a_1(D_i(t) - c_1)}} \tag{3}$$

where $D_i(t)$ denotes the distance between node i to a location of ideal cluster-head; a_1 that determines the shape of the function is set as -0.05; and c_1 that determines the position of the function is set as 125. Figure 3 shows this function versus $D_i(t)$. We use another sigmoid function to denote the possibility to be elected as a cluster head (versus remaining energy level),

$$f(E_i(t)) = \frac{1}{1 + e^{-a_2(E_i(t) - c_2)}} \tag{4}$$

where a_2 is set as 2 and c_2 is set as 2.5. Figure 4 shows this function versus $E_i(t)$. We define the possibility of each node to be selected as a cluster-head as

$$P_i(t) \triangleq f(E_i(t)) * g(D_i(t)) \tag{5}$$

IV. Analysis and Simulation Results

A. Experiment Setup

To evaluate the performances of modified LEACH discussed in the previous chapter, we presented these simulations by MATLAB. For a sensor network we make the following assumptions:

- The base station (BS) is located far from the sensors and immobile
- All nodes in the network are homogenous and energy-constrained.
- All nodes are able to reach BS.
- All nodes always have data to send.
- Symmetric propagation channel
- Cluster-heads perform data compression.

Our simulations consist of 100 nodes distributed randomly across a plain area of 1000x1000 meters as shown in Figure

5. The base station is located at position (500, 1750). Each node is equipped with 2 J of energy at the beginning of the simulation and an unlimited amount of data to send to the base station. Each non-cluster head node only needs to transmit a 200-bit message to its cluster-head once during a frame. Cluster-heads collect n 200-bit messages from n adjacent nodes and compress the data to $c \times n$ 200-bit messages that are transmitted to the base station, with $1 > c$ as the compression coefficient. For the experiments described in this paper, the compression coefficient is set as $c = 0.7$ and communication energy the energy for data aggregation is set as =5nJ/bit/signal.

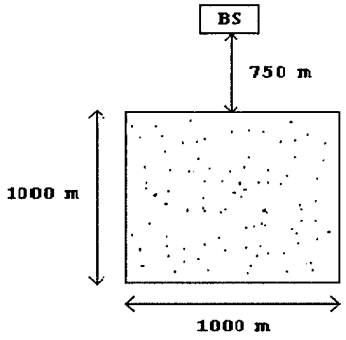


Fig. 5. Random 100-node topology for a 1000m×1000m network. BS is located at (500,1750), which is atleast 750m from the nearest node.

When there is only one cluster, the non-cluster-head nodes often have to transmit data very far to reach the cluster head node, draining their energy, and when there are more than five clusters, there is not as much local data aggregation being performed. For the experiments described in this paper, we set to five.

B. Nodes Begin with Equal Energy

For the first set of experiments, each node begins with 2 J of energy and an unlimited amount of data to send to the base station. Since each node begins with limited equal energy in these simulations, each node uses the probabilities in Eq. (1) to determine its cluster-head status at the beginning of each frame. We tracked the rate at which the data are transfer to the base station and the amount of energy required to get the data to the base station. Once a node runs out of energy, it is considered dead and can no longer transmit or receive data.

Figure 6 shows the total number of nodes that remain alive over the simulation time. The cluster-heads are uniformly distributed over the network to avoid them being located near the edges of the network or too close together. Besides, combine with the remaining energy level available in each node, this leads to a balanced energy consumption of all nodes. Therefore, all other nodes in the network die rapidly since the first node dies.

C. Nodes Begin with Unequal Energy

If nodes have unequal initial energies, the nodes with more energy should be cluster-heads more often than the nodes with

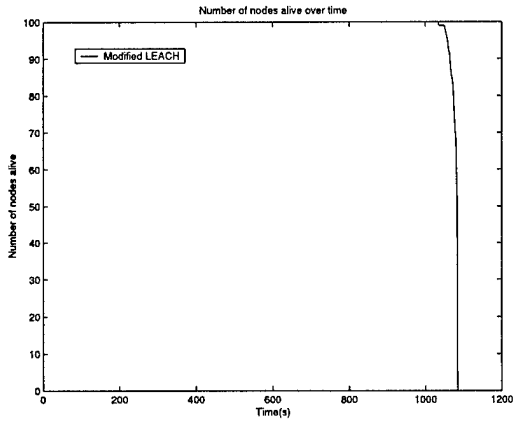


Fig. 6. Number of nodes alive over time, where each node with 2J of energy

less energy, to ensure that all nodes die at approximately the same time. In addition, we can take the factor of the distance between the non-cluster-head nodes and their cluster-head nodes in a cluster under consideration for reducing energy dissipation. Figures 7∼8 show the simulation results of LEACH and modified LEACH which include the factors of the remaining energy level and distance.

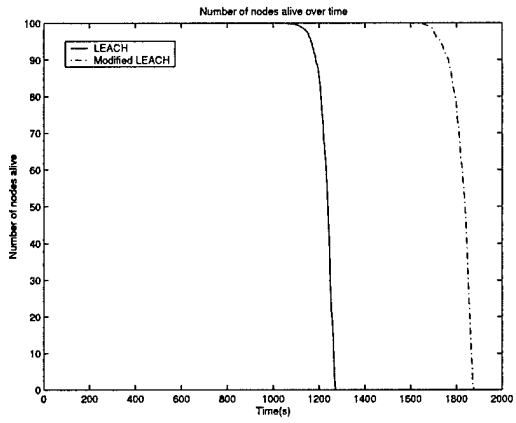


Fig. 7. Number of nodes alive over time, where each node with 2J∼5J of energy

To see how well the modification of LEACH's cluster-head selection can utilize any high-energy nodes in the network, we ran simulations with two scenarios. One scenario is the nodes in the network begin with 2∼5 J of energy as shown in Figure 7. The other scenario is the nodes in the network begin with 1∼10 J of energy as shown in Figure 8. The modified LEACH can take advantage of any high-energy nodes to extend the network lifetime. The results show that using the probabilities in Eq.(5), the network lifetime of the modified LEACH is much longer than LEACH, especially in the second scenario.

The definition of the lifetime of a sensor network is determined by the kind of service it provides. In some case, it is necessary that all nodes stay alive as long as possible, since network quality decreases considerably as soon as one

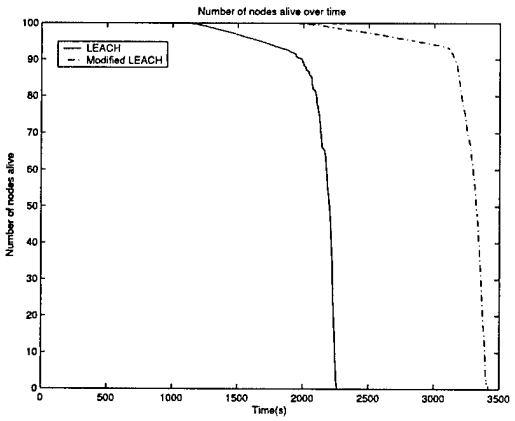


Fig. 8. Number of nodes alive over time, where each node with 1J∼10J of energy

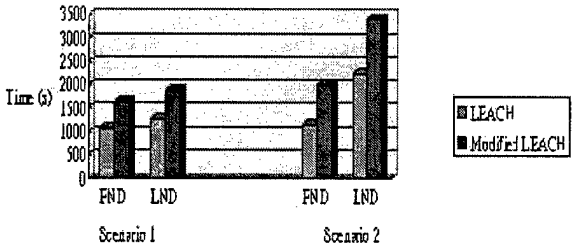


Fig. 9. The simulation results of the network lifetime

node dies. Scenarios for this case include intrusion and fire detection. In these scenarios it is important to know when the first node dies. The metric "First Node Dies (FND)" denotes an estimated value for this event of a specific network configuration. Besides, the overall lifetime of a sensor network can be determined by the metric "Last Node Dies (LND)". Therefore, we compare the modified LEACH and LEACH by using these metrics. FND increases by about 52 % and LND increases by about 49 % from Figure 7 where nodes begin with 2∼5 J of energy. FND increases by about 72 % and LND increases by about 51 % from Figure 8 where nodes begin with 1∼10 J of energy. These two graphs show that the network lifetime, which compares with LEACH,increases significantly when the bigger difference in energy capabilities of nodes in the network.

V. Conclusions

This paper focuses on reducing the power consumption of wireless microsensor networks. Consequently, a communication protocol named LEACH is modified to extend network lifetime. This paper has discussed two modifications of LEACH's stochastic cluster-head selection algorithm. We compare the modified LEACH and LEACH by using the metrics of "First Node Dies (FND)" and "First Node Dies (FND)". FND increases by about 52 % and LND increases by about 49 % when nodes begin with 2∼5 J of energy. FND increases by about 72 % and LND increases by about 51 % when nodes begin with 1∼10 J of energy. With these modifications of LEACH, the network lifetime can lengthen significantly as shown in Figure 9. Based on our MATLAB simulations described in the previous chapter, we are confident that the modified LEACH will outperform LEACH, in terms of energy dissipation,and system lifetime. Furthermore, an important quality of a LEACH network is maintained despite of the modifications: For the deterministic selection of cluster-heads only local and no global information is necessary to reduce the amount of transmitted data. The nodes themselves determine whether they become cluster-heads. A communication with the base station or an arbiter node is not necessary.

Acknowledgment

This work was supported by the U.S. Office of Naval Research (ONR) Young Investigator Program Award under Grant N00014-03-1-0466.

References

[1] S. Agarwal, et al, "Distributed power control in ad hoc wireless networks," *IEEE 12th International Symposium on Personal Indoor Mobile Radio Communications (PIMRC)*, San Diego, CA, Sept 2001.

[2] F. J. Block, and C. W. Baum, "An energy-efficient routing protocol for wireless sensor networks with battery level uncertainty," *IEEE Military Communications Conference*, Anaheim, CA, Oct 2002.

[3] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An application specific protocol architecture for wireless microsensor networks", *IEEE Transaction on Wireless Networking*, vol. 1, no. 4, pp 660∼669, Oct. 2002.

[4] Q. Li, J. Aslam, and D. Rus, "Online power-aware routing in wireless ad-hoc networks," *Proc. of Annual ACM/IEEE International Conf. on Mobile Computing and Networking (MobiCom)*, Rome, Italy, pp. 97-107, 2001.

[5] S. Lindsey, and C. S. Raghavendra, "PEGASIS: power-efficient gathering in sensor information systems," *IEEE Aerospace Conference*, March 2002.

[6] V. Rodoplu, and T. Meng, " Minimum energy mobile wireless networks," *IEEE J. Selected Areas in Communications*, vol. 17, no. 8, pp. 1333-1344, Aug 2000.

[7] A. Safwat, H. Hassanein, and H. Mouftah, "Power-aware fair infrastructure formation for wireless mobile ad hoc communications," *Proc. of Globecom'2001*, pp. 2832-2836, San Antonio, TX, Sept 2001.

[8] C. Schurgers, V. Tsiatsis, S. Ganeriwal, and M. Srivastava, "Optimizing sensor networks in the energy-latency-density design space," *IEEE Trans. on Mobile Computing*, vol. 1, no. 1, pp. 70-80, Jan-Mar 2000.

[9] S. Singh, M. Woo, and C. S. Raghavendra, "Power-aware routing in mobile ad hoc networks," *Proc. of Annual ACM/IEEE International Conf. on Mobile Computing and Networking (MobiCom)*, Dallas, TX, pp. 181-190, 1998.

[10] C.-K. Toh, "Maximum battery life routing to support ubiquitous mobile computing in wireless ad hoc networks," *IEEE Communications Magazine*, vol. 39, no. 6, pp. 138-147, July 2000.

[11] S.-L. Wu, Y.-C. Tseng, and J.-P. Sheu, "Intelligent medium access for mobile ad hoc networks with busy tones and power control," *IEEE J. Selected Areas in Communications*, vol. 18, no. 9, pp. 1647-1657, Sept 2000.

[12] Y. Xue and B. Li, "A location-aided power-aware routing protocol in mobile ad hoc networks," *Proc. of Globecom'2001*, pp. 2837-2841, San Antonio, TX, Sept 2001.

Secure Media Access Control (MAC) in Wireless Sensor Networks: Intrusion Detections and Countermeasures

Qingchun Ren
Department of Electrical Engineering
University of Texas at Arlington
416 Yates Street
Nedderman Hall, Rm 205
Arlington, TX 76019
Email: ren@wcn.uta.edu

Qilian Liang
Department of Electrical Engineering
University of Texas at Arlington
416 Yates Street
Nedderman Hall, Rm 518
Arlington, TX 76019
Email: liang@uta.edu

Abstract— **Current works on MAC protocols in Wireless Sensor Networks(WSN) mainly concentrate on optimizing the efficiency and fairness of common channel access. In this paper, we propose a secure MAC protocol improve the security of WSN, which is based on the RTS(Request to Send)/CTS(Clear to Send) mechanism. Our major contributions include: analyzed the security problems of RTS/CTS based MAC protocols; Designed the intrusion detection method using soft decision theory; discussed intrusion strategies and provided attack and defense simulation models.**

I. Introduction

A. DoS Attack

In Denial of Service(DoS)[1] attack, malicious users exploit the connectivity of the network to cripple the services provided by a victim site, by simply flooding a victim with many requests. A DoS attack can be either a single-source attack, originated only at one host, or a multi-source attack, in which multiple hosts cooperate to flood the victim with a barrage of attack packets. The latter is called Distributed Denial of Service (DDoS) attack[2]. In this paper, DoS attack is our target. Without proper security mechanisms, networks will be confined to limited, controlled environments, negating much of promise they hold. While DoS has been studied extensively for the wire-line networks, it is lack enough of research in WSN. Due to deployment in tactical battlefield missions, WSN[3] is susceptible to attacks by malicious intruders. Meanwhile, some salient features of WSN lay challenges in securing the security of message transmitted in the networks, such as wireless links, environment with relatively poor physical protection, dynamic topology and consisting of hundreds or even thousands of nodes.

DoS attack on WSN might attempt to disrupt/degrade the function of the whole network or might harm a specific node. DoS attack on WSN could be locating at Routing layer and MAC layer. Dos attack in routing layer would result in disruption of routing function, while in MAC layer, it could potentially disrupt channel access and might cause wast of bandwidth and power resources. Our research in this paper covers only the attacks in MAC layer

B. MAC Protocol

Wireless media is shared. This make nodes in wireless network can transmit at any point, which could cause contention over the common channel. MAC protocol is a set of rules or procedures to allow the efficient and fair use of this shared media. Referring to whether contention existed or not, there are two categories of MAC protocols. One is token-based, like FDMA, TDMA, CDMA, DBTMA[4]. Another is contention-based, such as MACA, WMACA, MACA/CD[4]. Because of the characteristics of WSN, the MAC protocols. which are based on contention and the RTS-CTS mechanism, are now widely used. In our algorithm, To make our method meet this trend, we choose this type of MAC protocols to discuss the security problem and design the countermeasures.

Some intrusion detection algorithms for wireless networks were proposed in[5], [6], [7]. All of them need special nodes to execute intrusion detection. Wired Equivalent Privacy(WEP) is one of the security protocols provided by IEEE 802.11[8] wireless standard to bring security into wireless networks. SPINS[9] is another security protocol for WSN.

The remainder of the paper is organized as follows: all possible security problems on MAC layer are analyzed in Section II. Our algorithm design is presented in Section III, including the intrusion detection method and countermeasures. Simulation results are given in Section IV and Section V concludes this paper.

II. Attacks on WSN's MAC Protocols

Many MAC protocols in WSN just consider the efficiency and fairness of utilizing the common channel. They assume that in the whole network each node strictly complies with the same rule to access the media and get the right to hold the channel. For these reasons, many MAC protocols of WSN are very vulnerable. We classify the attacks on MAC protocols

into three categories: collision attack,exhaustion attack and unfairness attack. Definitions are presented as follows:

A. Collision Attack

As discussed above, each node could inform its neighbors that he has some data to send or receive by exchanging RTS/CTS control packets. Neighbor nodes could detect that the public channel is busy, and they would back off their sending even if they have some data packets to send. Using this mechanism, the collision only happens in the exchanging period of RTS and CTS packets, which means the data packet sending process is a non-collision process. In addition, each node will check whether the channel is busy or idle before sending RTS and CTS packets. That's why the probability of collision is very low. Under the condition, when there is a packet transmitting on channel, adversaries can easily conduct attacks through sending out some packets to disrupt it(such as data packs, control packets sent by normal nodes). We call this kind of attack collision attack.

B. Unfairness Attack

For most RTS/CTS-based MAC protocols, each node has the same priority to get the common channel. The rule is that the first tried node gets hold of the channel. Besides, all other nodes have to wait for a random length time before trying to transmit packets. This rule could ensure that every node accesses common channel fairly. Adversaries could utilize these characteristics to attack the network. They send out packets just waiting for a very short time or without waiting. This causes the common channel used more by adversaries than by normal nodes. This is what we called unfairness attack.

C. Exhaustion Attack

RTS/CTS based MAC protocols are sender invitation MAC protocols. That is, when a sender sends out RTS control packet to start a transmission, the receiver has to acknowledge the invitation with CTS control packet if it is available. Since adversaries are also normal nodes, the receiver can't exactly distinguish whether the RTS packet was sent by normal nodes or by adversaries. Under this condition, adversaries can attempt to retransmit RTS control packets to normal nodes repeatedly, enforcing receiver to acknowledge them incessantly. These kinds of abnormal retransmissions could culminate in the exhaustion of battery resources of receivers. We name this kind of attack exhaustion attack.

III. Our Intrusion Detection and Strategies Algorithm

Traditional security mechanisms, such as authentication protocols, digital signature, and encryption, still play important roles in achieving confidentiality, integrity, authentication, and non-repudiation of communication in wireless networks. However, these mechanisms only act as the first line of defense. They are not strong enough to make WSN be immune for all kinds of attacks. Especially, when some normal nodes were captured and reprogrammed by enemies, they would get the legal right to access the network[10]. We aim at improving the safety of MAC layer through adding our algorithm to these RTS/CTS based MAC protocols. There are two function modules in our algorithm: intrusion detection and intrusion defense. These two modules are executed by each node separately and automatically. Cooperations among nodes are not required, therefore it is a distributed method. In addition, no extra hardware is needed. Considering this, our new algorithm is not expensive to apply.

A. Intrusion detection

Once the attackers obtain the authorization to access the network, they could attack the network using one of the three types of above-mentioned attacks. Through simulation, we observed that these attacks result in some abnormal changes on the performances of the network. For example, packet collision ratio becomes very high, successful data packet transmission ratio decreases steeply, and so on. In our algorithm, unusual changes of sensitive data elements are chosen to trigger the intrusion detection. We choose following statistics as intrusion indicators:

- Collision Ratio (R_c): R_c is the collision times detected by a node per second.
- Probability of Data Packet Successful Transmission (P_{st}): We define a successful transmission as a correct sending and receiving process of data packet. P_{st} is the ratio of the number of successful data packets transmitted to the total number of data packet transmitted.
- Data Packet's Waiting-Time (T_w): T_w is the time of data packet in MAC layer buffer waiting for transmission.
- RTS Packets Arrival Ratio (R_{RTS}): R_{RTS} is the number of RTS packets received successfully by a node per second.

We collect the values of all indicators periodically, and estimate the intrusion probabilities for each of them. According to these probabilities, we can conclude whether there is an intrusion or not. This is a soft decision process. The advantage of using soft decision is that we can effectively reduce the chance to make fault decision, which is caused by very small fluctuation of any indicator's value. Our decision function is as following:

$$y(x) = \frac{1}{1 + \exp[-A \times (x - C)]} \tag{1}$$

Notes:

- Parameter "A" determines the slop of curve. The bigger the value is , the steeper the slop of the curve is;
- Parameter "C" determines the center of curve.
- In our experiments, we adaptively adjust the shape of curve through adjusting parameter A and C. The adjust method will be described in the following part.

The intrusion probabilities got:

- Probability of collision attack (P_c): P_c is the probability of collision attack found. It directly relates to R_c;

- Probability of exhaustion attack (P_e): P_e is the probability of exhausion attack found. It directly relates to R_{RTS};
- Probability of unfairness attack (P_u): P_u is the probability of unfairness attack found. It directly relates to T_w;
- Probability of total (P_t): P_t directly relates to P_st.

We choose the threshold (P_{th}) for these four probabilities. If the combined probability of Pt and P_c, P_e or P_u is bigger than P_{th}, the intrusion detection module announces that there is an attack found. Otherwise, there is no attack found. When the decision is an intrusion existing, the defense part will start to make countermeasures. The relationships are described in Figure 1.

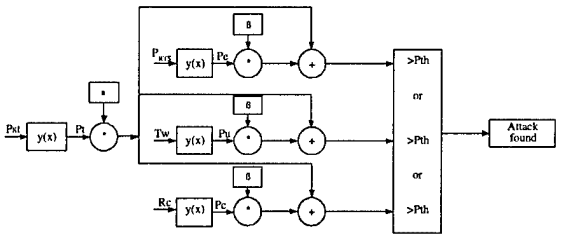


Fig. 1. Intrusion Probability Process Flow

Note: α, β is the weight. They are decimal numbers between 0 and 1.

Power is one of the most important resources for WSN. So generally the traffic type of this network is almost like pulse. That is to say, the nodes in the whole network stay at sleep mode or idle mode in most of the simulation time. For this reason, the intrusion indicators we are interested in are time variances. In sleep mode or idle mode, the R_c, T_w, R_{RTS} are much lower than those in transmitting/receiving mode. The decision function should be adaptive. For if it is fixed, two cases might take place:

- The Probability of successful detection (P_d) is too high and Probability of fault detection (P_{fd}) is too high.
- P_d is too low and P_{fd} is too low.

Note:

A successful detection is an intrusion alarm that is done during the attacker's intrusion period. P_d is the ratio of successful detection times to total attack times. A fault detection is an intrusion alarm that is done during no intrusion period. P_{fd} is the ratio of fault detection times to total times without attack.

We use the steepest descent algorithm[11] to train parameter A and C adaptively.

Cost function:

$$J(x) = (y_d - y)^2 \tag{2}$$

where y_d is the desired value of intrusion probability, y is the actual value.

$$C(k+1) = C(k) + \alpha \times \frac{\partial J}{\partial C} \tag{3}$$

$$A(k+1) = A(k) + \alpha \times \frac{\partial J}{\partial A} \tag{4}$$

where

$$\frac{\partial J}{\partial C} = 2\,(y_d - y)\,\frac{-A(k)\exp\{-A(k)\times[x - C(k)]\}}{\{1+\exp\{-A(k)\times[x-C(k)]\}\}^2} \tag{5}$$

$$\frac{\partial J}{\partial A} = 2\,(y_d - y)\,\frac{A(k)}{\{1+\exp\{-A(k)\times[x-C(k)]\}\}^2} \tag{6}$$

(k=1, 2, 3...)

Notes:

- We calculate the intrusion probability periodically;
- α is the training factor. Its value locates between 0 and 1;
- In our algorithm, we assume that each node uses some method to get the y_d through other method. For example, getting it from the base station of local cluster.

B. Defense part

When intrusions are found, the defense part starts to work, using some countermeasure to reduce the effects of attackers on the network. From the analysis above, we found that it is a waste of energy or unsafe action for the node to try to transmit information during intrusion period. The reason is, the transmission is almost unsuccessful or spied by attackers when enemies attack the network. Besides, there is no cooperation among nodes, and no center control stations existed in the network. Thus, stopping transmission and receiving at this time is a very easy and valuable method to void the intrusion. Our countermeasure is to force the node switch to sleep mode for a period of time, when it found the intrusion happen. And each node schedules its sleep plan individually.

IV. Simulation and Discussion

In this section, we quantify and evaluate attacks on the MAC layer, and the efficiency of our detection and defense algorithm. We use OPNET software as our simulations tool. The analysis is complicated by Packet relay, mobility, and randomness of the topology. So we configure that the topology is fixed during simulations, and the communication range of each node in the network is limited, however in the small zone, e.g.inside a cluster, each node can communicate directly with any other node belonging to the same zone. We separately test the effects of different types of intrusion(i.e. collision attack, exhaustion attack or unfairness attack) on the performances of network. In each simulation, there is only one type of attack introduced, and in each cluster, there is one attacker. We assume that the enemies have captured normal nodes and transformed them into attackers successfully. In our simulations, we make attackers starting the intrusion at the random time and the attack lasting for a random length of time. We detect following parameters to testify the effects of our algorithm:

- P_{st}, P_d, P_{fd};
- Average energy consumption (E_{av})(J/Pk): E_{av} is the energy consumed per successful transmission data packet.

- Time of first node dead (T_s)(Second): When the energy of a node used out, we define this node dead. T_s is the time of the first node, in the network, consumes its power out.

In our simulation, each node has limited power. The initial energy of each node is $2J$. We use the same energy consumption model as that in [12]. When node stays at sleep mode, we assume that there is no energy consumed. We use equation(7) to calculate the energy consumption of receiving a packet, and use equation(8) to calculate the energy consumption of transmitting a packet.

$$E_{Rx} = l \times E_{elec} \tag{7}$$

$$E_{Tx} = l \times E_{elec} + l \times e_{fs} \times d^2 \tag{8}$$

Separately adding collision attack, exhaustion attack and unfairness attack into network, we design three groups of simulation scenarios. In each group of simulations, we compare the performances of traditional network with the network using our new security algorithm.

A. Adding collision attack to each cluster in the whole network. We get these results, shown in figure 2 and figure 3.

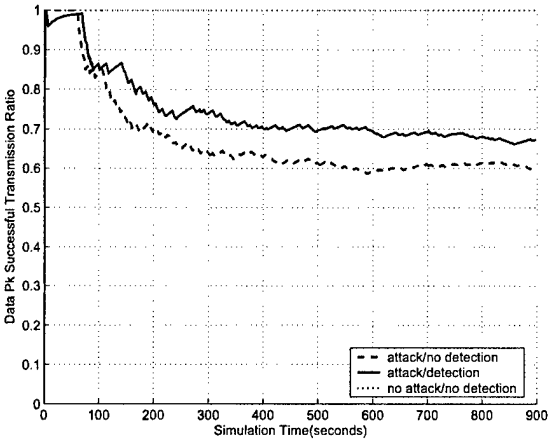


Fig. 2. Probability of Data Packet Successful Transmission

B. Adding unfairness attack to each cluster in the whole network. We get these results, shown in figure 4 and figure 5.

C. Adding exhaustion attack to each cluster in the whole network. We get these results, shown in figure 6 and figure 7.

In Table 1, we provide the time that first node dies under three different types of attacks. The time is 200s under no attack condition.

For three different types of attack, the probability of fault detection of our algorithm is 0, and the probability of successful detection is 100%.

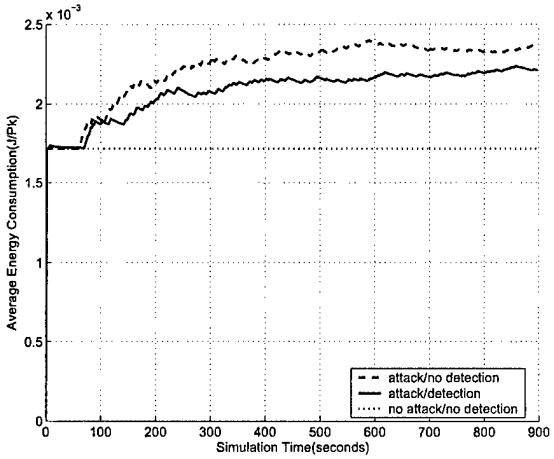


Fig. 3. Average Energy Consumption

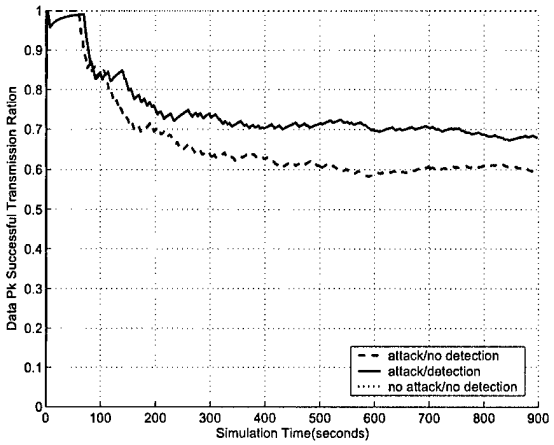


Fig. 4. Probability of Data Packet Successful Transmission

Observing simulation results, our detection algorithm detects all collision attack, exhaustion attack and unfairness attack successfully when intrusion happen. At the same time, we don't make any fault alarm when no intrusion existed. Furthermore, our defense algorithm schedule protection plan successfully. According to figure 2,4 and 6, probability of success transmission increases about 10%. According to figure 3,5 and 7, the average energy consumption decreases about 5% per packet. According to Table 1, the first node dead time is extended for around 140 seconds. That means the lifetime of whole network becomes longer.

V. Conclusions

In this paper, we studied the security on MAC layer of WSN. We applied intrusion detection and defense into original RTS/CTS-based MAC protocol. Our algorithm can avoid the attack and energy waste to some degree. Furthermore, this algorithm doesn't require any additional hardware or cooper-

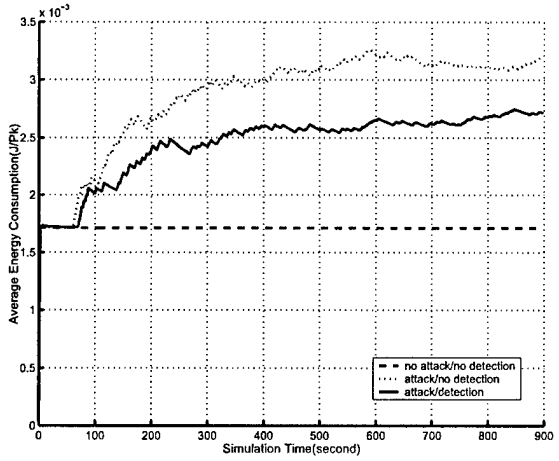


Fig. 5. Average Energy Consumption

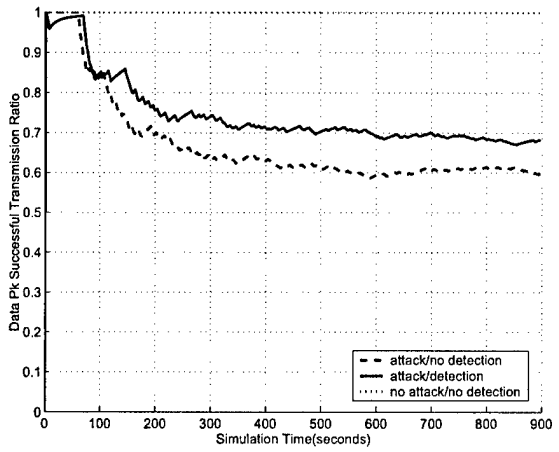


Fig. 6. Probability of Data Packet Successful Transmission

ation among nodes. Simulation results show that our protocol for WSN works very well.

ACKNOWLEDGEMENT

This work was supported by the U.S. Office of Naval Research (ONR) Young Investigator Program Award under Grant N00014-03-1-0466.

The authors would like to thank Ms. Haining Shu for reviewing the whole paper and providing some comments, most of which we have incoporated into the final version.

REFERENCES

[1] A. D. Wood, J. A. Stankovic, " Denial of service in sensor networks ," *IEEE JNL* , Vol 35, Issue 10, Oct. 2002 pp54-62

[2] A. D. Wood, J. A. Stankovic, " Defeating distributed denial of service attacks ," *IEEE JNL* , Vol 2, Issue 4, July-Aug. 2000 pp36-42

[3] V. Rajaravivarma, Y. Yang, T. Yang, " An overview of Wireless Sensor Network and applications ," *Proceedings of the 35th Southeastern Symposium*, March 2003 pp432-436

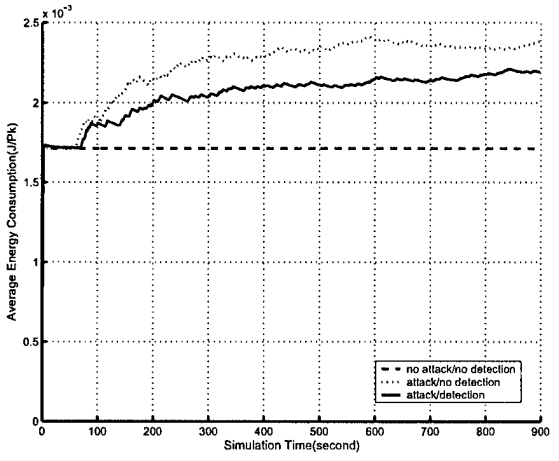


Fig. 7. Average Energy Consumption

TABLE I
TIME OF FIRST NODE DEAD

	CollisionAttack		UnfairnessAttack		ExhaustionAttack	
	NoDetect	Detect	NoDetect	Detect	NoDetect	Detect
Ts	126s	272s	126s	276s	108	230s

[4] C. K. Toh, " Ad Hoc Mobile Wireless Networks: Protocols and Systems ," ISBN 0-13-007817-4

[5] H. Chan, A. Perrig, " Security and Privacy in Sensor Networks ," Security Oct. 2003, pp.103-105

[6] M. K. Chirumanilla, B. Ramamurthy, " Agent Based Intrusion Detection and Response System for Wireless LANs ," *ICC '03. IEEE International Conference on* , Vo. 1 , 2003, pp.492 - 496

[7] J. E. Dickerson, J. Juslin, O. Koukousoula, J. A. Dickers, " Fuzzy Intrusion Detection ," *Joint 9th IFSA World Congress and 20th NAFIPS International Conference*, Vo. 4, 2001, pp.2165-2170

[8] O. Kachirski, R. Guha, " Effective Intrusion Detectin Using Multiple Sensors in Wireless Ad Hoc Networks ," *SIGCOMM'03*, Aug. 2003

[9] " 802.11 Standard ," *http://grouper.ieee.org/groups/802/11*

[10] A. Perrig, R. Szewczyk, J. D. Tygar, D. Culler, " SPINS: Security Protocols for Sensor Networks ," Wireless Networks 8, pp.521-534, 2002

[11] J. M. Mendel, " Uncertain Rule-Based Fuzzy Logic Systems: Introduction and New Directions ," ISBN: 0-13-040969-3

[12] W. B. Heinzelman, A. P. Chandrakasan, H. Balakrishnan, " An Application-Specific Protocol Architecture for Wireless Microsensor Networks ," *IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS*, Vol. 1, NO.4, OCT. 2002

[13] E. H. Mamdani, " Applications of fuzzy logic to approximate reasoning using linguistic systems", *IEEE Trans. on Systems, Man, and Cybernetics*, vol. 26, no. 12, pp. 1182-1191, 1977.

[14] J. M. Mendel, "Fuzzy Logic Systems for Engineering : A Tutorial," *Proceedings of the IEEE*, vol. 83, no. 3, pp. 345-377, March 1995.

[15] J. M. Mendel, *Uncertain Rule-Based Fuzzy Logic Systems*, Prentice-Hall, Upper Saddle River, NJ, 2001.

Secure Media Access Control in Wireless Sensor Networks: Intrusion Detections and Strategies

Qingchun Ren
Department of Electrical Engineering
University of Texas at Arlington
416 Yates Street
Nedderman Hall, Rm 205
Arlington, TX 76019
Email: ren@wcn.uta.edu

Qilian Liang
Department of Electrical Engineering
University of Texas at Arlington
416 Yates Street
Nedderman Hall, Rm 518
Arlington, TX 76019
Email: liang@uta.edu

Abstract— **Current works on Media Access Control(MAC) protocols in Wireless Sensor Networks(WSN) mainly concentrate on optimizing the efficiency and fairness of common channel access. In this paper, we propose a secure MAC protocol to improve the security of WSN, which is based on the RTS(Request to Send)/CTS(Clear to Send) handshake mechanism. Our major contributions include: analyzed the security problems of RTS/CTS based MAC protocols; Designed the intrusion detection method using fuzzy logical theory; Discussed intrusion strategies and provided attack and defense simulation models.**

I. Introduction

A. DoS Attack

In Denial of Service(DoS)[1] attack, malicious users could exploit the connectivity of the network to cripple the services provided by a victim site, by simply flooding a victim with many requests. A DoS attack can be either a single-source attack, originated only at one host, or a multi-source attack, in which multiple hosts cooperate to flood the victim with a barrage of attack packets. The latter one is called Distributed Denial of Service (DDoS) attack[2]. In this article, single-source DoS attack is our target. Dos attack is critical in most security system. Without proper security mechanisms, networks will be confined to limited, controlled environments, and negat much of promise they hold. While DoS has been studied extensively for the wire-line networks, such as in Internet. It is lack enough of research in WSN. Meanwhile, some salient features of WSN lay challenges in securing the security of messages transmitted over the networks. For example, using wireless links makes WSN susceptible to link attacks ranging from passive eavesdropping, active impersonation, message replay, to message distortion. Second, nodes, roaming in a hostile environment with relatively poor physical protection, have non-negligible probabilities of being compromised. Third, WSN may be dynamic because of frequent changes both in its topology and its membership. Finally, WSN may consist of hundreds or even thousands of nodes.

DoS attack on WSN might attempt to disrupt/degrade the function of the whole network or might destroy a specific node. These attacks can either be internal - attack carried by people within the organization - or external - attack carried by people outside the organization. DoS attack on WSN could be locating at Routing layer and MAC layer. On routing layer, Dos attack would results in disruption of routing function. While, on MAC layer, it could potentially disrupt channel access and might cause wast of bandwidth and power resources. Our research in this paper covers only the attacks on MAC layer

B. MAC Protocol and Secure Protocol

Wireless media is shared by all nodes in the network. This make all the nodes in wireless network can transmit at any point, which could cause contention over the common channel. MAC protocol is a set of rules or procedures to allow the efficient and fair use of this shared media. Referring to whether contention existing or not, there are two categories of MAC protocols. One is token-based, like FDMA, TDMA, CDMA, DBTMA[4]. The other is contention-based, such as MACA, WMACA, MACA/CD[4]. Because of the characteristics of WSN, the MAC protocols, which are based on contention, carrier sense and RTS-CTS mechanism, are now widely used. To make our method meet this trend, we choose this type of MAC protocols to discuss the security problem and design our intrusion detection and strategies.

In the literature, some intrusion detection algorithms for wireless networks were proposed in[5], [6], [7]. They all need additional nodes for to execute intrusion detection. Wired Equivalent Privacy(WEP) is one of the security protocols provided by IEEE 802.11[8] wireless standard to bring security into wireless networks. Its main objective is to protects the data that is transmitted over wireless links from malicious eavesdroppers. SPINS[9] is another security protocol for WSN. It has two secure building blocks: SNEP and μTESLA. SNEP includes: data confidentiality, two-party data authentication, and evidence of data freshness. μTESLA provides authenticated broadcast for severely resource-constrained environments.

The rest of this paper is organized as follows: almost possible security problems on MAC layer are analyzed in Section II. Our algorithm design is presented in Section III, including the intrusion detection method and countermeasures. Simulation results are given in Section IV and Section V concludes this paper.

II. Attacks on WSN's MAC Layer

Many MAC protocols, currently proposed, for WSN mainly concentrated on how to utilize the common channel efficiently and fairly when they are designed. They also assume that in the whole network each node strictly complies with the same rule, MAC protocol, to access the media and get the right to hold the channel for a period of time. For these reasons, MAC lay of WSN is very vulnerable for attackers. We classify the Dos attacks on MAC layer into three categories: collision attack, exhaustion attack and unfairness attack. The security risks and related attack are presented in the following parts.

A. Collision Attack

As mentioned above, before data packets transmission, there is a RTS-CTS packets exchanging process. Sender and receiver utilize RTS and CTS packet to inform its neighbors that the channel has been held by them. On neighbor nodes side, when they detect the public channel is busy, they would back off their sending even if there are some data packets to send. Using this mechanism, the collision only happens in the exchanging period of RTS and CTS packets, which means the data packet sending process is a non-collision process. That's why data packets could be successfully and efficiently transmitted over the network. Under the condition, when there is a packet(i.e. data packs, control packets sent by normal nodes) transmitting on channel, adversaries can easily conduct attacks through sending out some packets to disrupt it. We call this kind of attack collision attack.

B. Unfairness Attack

For most RTS/CTS-based MAC protocols, all other nodes have to wait for a random length time before trying to hold channel, and the first successfully tried node gets hold of the channel. This procedure could ensure every node accesses common channel fairly. Based on this characteristics, adversaries could occupy the channel for an unreasonably long time when they found the channel is idle. This could cause the common channel used more by adversaries than by normal nodes. This is what we called unfairness attack.

C. Exhaustion Attack

RTS/CTS based MAC protocols are sender invitation MAC protocols. That is, when a sender sends out RTS control packet to start a transmission, the receiver has to acknowledge the invitation with CTS control packet if it receives this invitation successfully. Since adversaries are transformed from normal nodes, the receiver can't exactly distinguish whether the RTS packet was sent by normal nodes or by adversaries. Under this condition, adversaries can attempt to retransmit RTS control packets to normal nodes repeatedly, enforcing receiver to acknowledge them incessantly. These kinds of abnormal retransmissions could culminate in the exhaustion of battery resources of receivers. We name this kind of attack exhaustion attack.

III. Our Intrusion Detection and Strategies Algorithm

Traditional security mechanisms, such as authentication protocols, digital signature, and encryption, still play important roles in achieving confidentiality, integrity, authentication, and non-repudiation of communication in wireless networks. However, these mechanisms could only act as the first line of defense. They are not strong enough to make WSN be immune to all kinds of attacks. Especially, when some normal nodes were captured and reprogrammed by enemies, they could access the network legally[10].

In this section, we describe our secure system. Figure 1 shows the structure of it. Through adding two special modules, intrusion detection module and intrusion defense module, into these RTS/CTS based MAC protocols, we improves the safety of MAC layer. The basic idea behind the algorithm is that,intrusion module of each node frequently monitors a serial of sensitive network performance indicators, then according to these statistics' values, the intrusion module make the decision, i.e. whether the intrusion exsited or not. If intrusion is found, the defense module of each node schedules the countermeasure to reduce the destory of the attacker. After a period of sleep, the node would wake up and make intrusion detection again. Therefore our algorithm is a distributed method, it doesn't based on cooperation among nodes. Furthermore, our algorithm is not expensive to be utilized by existed MAC protocols, because there is no extra hardware needed.

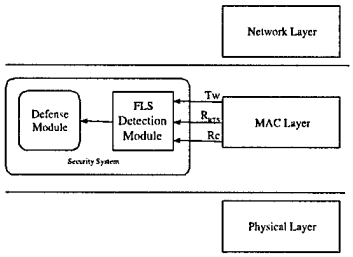


Fig. 1. The structure of our security system.

A. Intrusion Detection Using Fuzzy Logic Systems

- Overview of Fuzzy Logic Systems

  Figure 2 shows the structure of a fuzzy logic system (FLS) [14]. When an input is applied to a FLS, the inference engine computes the output set corresponding to each rule. The defuzzifer then computes a crisp output from these rule output sets. Consider a p-input 1-output FLS, using singleton fuzzification, *center-of-sets* defuzzification [15] and "IF-THEN" rules of the form [13]

  $$R^l : \text{IF } x_1 \text{ is } \mathrm{F}_1^l \text{ and } x_2 \text{ is } \mathrm{F}_2^l \text{ and } \cdots \text{ and } x_p \text{ is } \mathrm{F}_p^l, \text{ THEN } y \text{ is } \mathrm{G}^l.$$

  Assuming singleton fuzzification, when an input $\mathbf{x}' = \{x_1', \ldots, x_p'\}$ is applied, the degree of firing corresponding to the lth rule is computed as

  $$\mu_{\mathrm{F}_1^l}(x_1') \star \mu_{\mathrm{F}_2^l}(x_2') \star \cdots \star \mu_{\mathrm{F}_p^l}(x_p') = \mathcal{T}_{i=1}^{p} \mu_{\mathrm{F}_i^l}(x_i') \quad (1)$$

where $\star$ and $\mathcal{T}$ both indicate the chosen t-norm. There are many kinds of defuzzifiers. In this paper, we focus, for illustrative purposes, on the height defuzzifier [15]. It computes a crisp output for the FLS by first computing the height, $\bar{y}^l$, of every consequent set G^l, and, then computing a weighted average of these heights. The weight corresponding to the lth rule consequent height is the degree of firing associated with the lth rule, $\mathcal{T}_{i=1}^{p}\mu_{F_i^l}(x_i')$, so that

$$y_h(\mathbf{x}') = \frac{\sum_{l=1}^{M}\bar{y}^l\mathcal{T}_{i=1}^{p}\mu_{F_i^l}(x_i')}{\sum_{l=1}^{M}\mathcal{T}_{i=1}^{p}\mu_{F_i^l}(x_i')} \quad (2)$$

where M is the number of rules in the FLS. In this article, we design a FLS for intrusion detection.

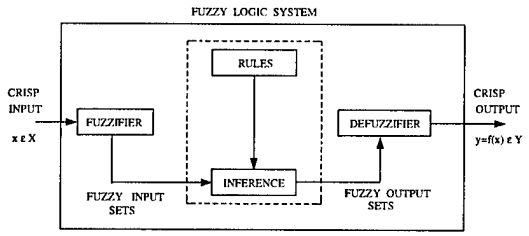


Fig. 2. The structure of a fuzzy logic system.

- Intrusion Detection
  Once the attackers obtain the authorization to access the network, they could attack the network using one of the three types of above-mentioned attacks. We observed that different attacks would result in different abnormal changes on the performances of the network. When the collision attacker intrudes the network, the collision on the channel and the average waiting time increase steeply. For unfairness attack, the average waiting time becomes much longer than normal value. For the exhaustion attacks, the amount of RTS packets received by a node per second and the average waiting time beyond the normal range. In our algorithm, these unusual changes of sensitive data elements are chosen to trigger the intrusion detection. The intrusion is detected based on three descriptions: RTS arrival ratio, collision ratio, and average waiting time for data packet.
  - Collision Ratio (R_c): R_c is the collision number detected by a node per second.
  - Average Waiting-Time (T_w): T_w is the time of data packet in MAC layer buffer waiting for transmission.
  - RTS Arrival Ratio (R_{RTS}): R_{RTS} is the number of RTS packets received successfully by a node per second.

  The linguistic variables used to represent the RTS arrival ratio and Collision ratio were divided into two levels: *Low* and *High*; and those to represent its average waiting time were divided into two levels: *Short* and *Long*. The cosequent - the possibility that this node finds intrusion attack - was divided intro 5 levels, *Very low*, *Low*, *Moderate*, *High* and *Very high*. We use trapezoidal membership functions(MFs) to represent *Low*, *High*, *Short*, *Long*, *Very low*, and *Very high*; and triangle MFs to represent *Moderate*, *Low*, and *High*. We show these MFs in Fig.3 and Fig. 4.

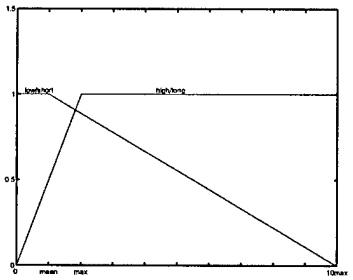


Fig. 3. Antecedent Membership Function

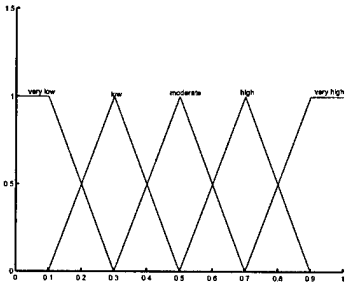


Fig. 4. Consequent Membership Function

Based on the facts that when any types of attacker(i.e. collision attack, exhaustion attack, unfairness attack) intrudes the network, the collision ratio, RTS arrival ratio and average waiting time would become extremly high/long. Stronger the intrusion is, the bigger the value of the collision ratio becomes, RTS packets arrival ratio and average waiting time are. We design a fuzzy logic system using rules such as:
R^l:IF *collision ratio*(x_1) *of a node detected* is F_l^1, *average waiting time*(x_2) *of a node collected* is F_l^2, and *RTS arrival ratio*(x_3) *of a node received* is F_l^3, THEN *the possibility that a intrusion found by this node*(y) is G^l.
Where l = 1,2,...,8. We summarize all the rules in Table 1.
For every input(x_1,x_2,x_3), the output is computed using

$$y(x_1,x_2,x_3) = \frac{\sum_{l=1}^{8}\bar{y}^l\mu_{F_1^l}(x_1)\mu_{F_2^l}(x_2)\mu_{F_3^l}(x_3)}{\sum_{l=1}^{8}\mu_{F_1^l}(x_1)\mu_{F_2^l}(x_2)\mu_{F_3^l}(x_3)} \quad (3)$$

By repeating these calculations for all x_i, we obtain a hypersurface y(x_1,x_2,x_3). The height of the five fuzzy sets depicted in Fig 3 are $\bar{y}^1$=0.1, $\bar{y}^2$=0.3, $\bar{y}^3$=0.5, $\bar{y}^4$=0.7, $\bar{y}^5$=0.9.

TABLE I

THE RULES FOR INTRUSION DETECTION. ANTECEDENT 1 IS COLLISION RATE, ANTECEDENT 2 IS AVERAGE WAITING TIME, ANTECEDENT 3 IS RTS ARRIVAL RATE, AND CONSEQUENT IS THE POSSIBILITY THAT INTRUSION ATTACK FOUND.

Rule	*Antecedent1*	*Antecedent2*	*Antecedent3*	*Consequence*
1	*Low*	*Low*	*Low*	*VeryLow*
2	*Low*	*Low*	*High*	*Moderate*
3	*Low*	*High*	*Low*	*Moderate*
4	*Low*	*High*	*High*	*High*
5	*High*	*Low*	*Low*	*Moderate*
6	*High*	*Low*	*High*	*Low*
7	*High*	*High*	*Low*	*High*
8	*High*	*High*	*High*	*VeryHigh*

B. Defense

When intrusions are found, the defense module starts to work, using some countermeasure to reduce the effects of attackers on the network. From the analysis above, we found that it is a waste of energy or unsafe action for the node to try to transmitting or receiving information during intrusion period. The reason is, the transmiting or receiveing is almost unsuccessful or spied by attackers when enemies attack the network. Besides, there is no center control stations in the network, and we don't hope to utilize the cooperation among nodes. Thus, stopping transmitting and receiving at this time is a feasible method to avoid the intrusion. Our countermeasure is to force the node switch to sleep mode for a period of time, when it finds the intrusion happen. And each node schedules its sleep plan individually.

IV. SIMULATION AND DISCUSSION

In this section, we quantify and evaluate attacks on the MAC layer, and the efficiency of our detection and defense algorithm. We use OPNET software as our simulations tool. The analysis is complicated by packet relay, mobility, and randomness of the topology. So we assume that the topology is fixed during simulations, and the communication range of each node in the network is limited. However in the small zone, e.g. inside a cluster, each node can communicate directly with any other node belonging to the same zone. We separately test the effects of different types of intrusion(i.e. collision attack, exhaustion attack or unfairness attack) on the performances of network. In each simulation, there is only one type of attack introduced, and in each cluster, there is only one attacker. We assume that the enemies have captured normal nodes and transformed them into attackers successfully. In our simulations, we make attackers start the intrusion at the random time and the attacks last for a random length of time. We detect following parameters to testify the effects of our algorithm:

- The Probability of successful detection (P_d):
  A successful detection is an intrusion alarm that is done during the attacker's intrusion period. P_d is the ratio of successful attack detectionsto total attacks.
- Probability of fault detection (P_{fd}):
  A fault detection is an intrusion alarm that is done during no intrusion period. P_{fd} is the ratio of fault attack detections to total moments without attack.
- Rate of data packet successful transmission(R_{st}):
  We define a success transmission as a correctly sending and receiving process of data pacet. R_{st} is the ratio of the number of successful data packet transmitted to the total number of data packet transmitted.
- Average energy consumption (E_{av})(J/Pk):
  E_{av} is the energy consumed per successful transmission data packet.
- Time of first node dead (T_s)(Second):
  When the energy of a node used out, we define this node dead. T_s is the time of the first node, in the network, consumes its power out.

In our simulation, each node has limited power. The initial energy of each node is $2J$. We use the same energy consumption model as that in [12]. When node stays at sleep mode, we assume that there is no energy consumed. We use equation(4) to calculate the energy consumption of receiving a packet, and use equation(5) to calculate the energy consumption of transmitting a packet.

$$E_{Rx} = l \times E_{elec} \tag{4}$$

$$E_{Tx} = l \times E_{elec} + l \times e_{fs} \times d^2 \tag{5}$$

Separately adding collision attack, exhaustion attack and unfairness attack into network, we design three groups of simulation scenarios. In each group of simulations, we compare the performances of traditional network with the network using our secure MAC algorithm.

A. Adding collision attack to each cluster in the whole network. We get these results, shown in figure 5 and figure 6.

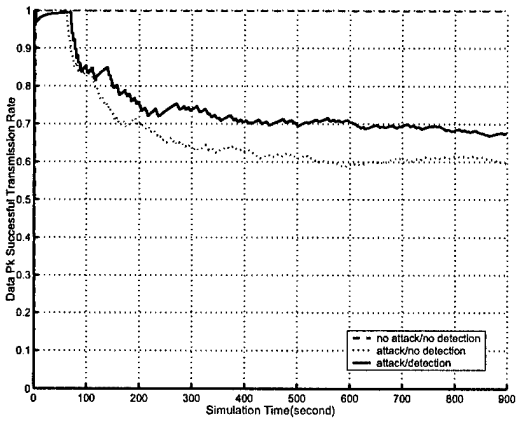


Fig. 5. Rate of Data Packet Successful Transmission

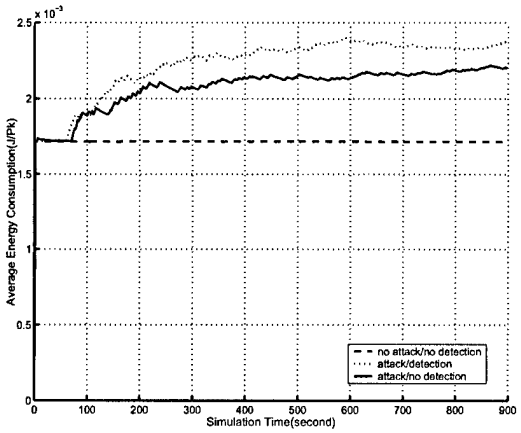


Fig. 6. Average Energy Consumption

B. Adding unfairness attack to each cluster in the whole network. We get these results, shown in figure 7 and figure 8.

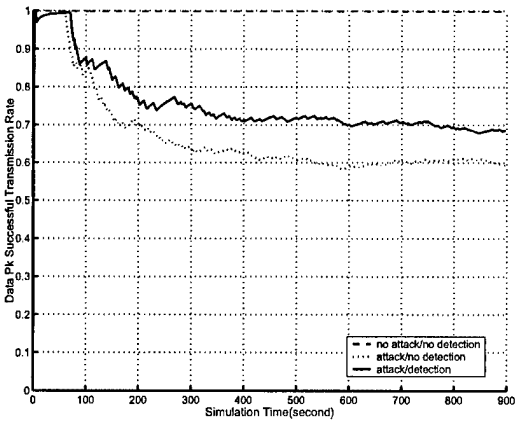


Fig. 7. Rate of Data Packet Successful Transmission

C. Adding exhaustion attack to each cluster in the whole network. We get these results, shown in figure 9 and figure 10.

In Table 2, we provide the time that first node dies under three different types of attacks. The time is 200s under no attack condition.

TABLE II
TIME OF FIRST NODE DEAD

	CollisionAttack		UnfairnessAttack		ExhaustionAttack	
	NoDetect	Detect	NoDetect	Detect	NoDetect	Detect
Ts	126s	271s	107s	229s	126	275s

For three different types of attack, the probability of fault

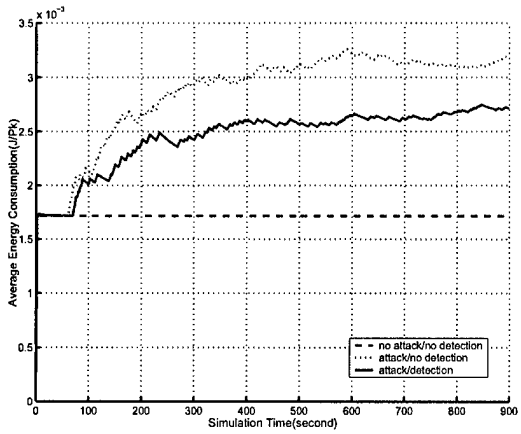


Fig. 8. Average Energy Consumption

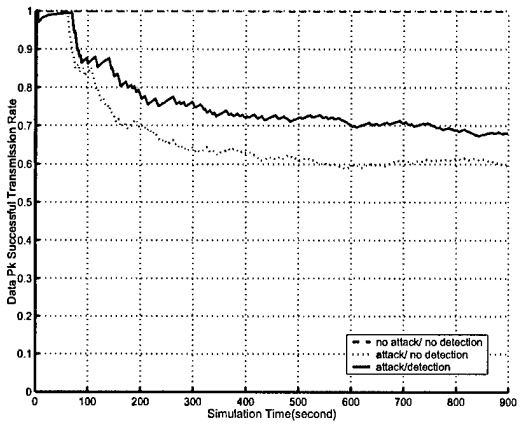


Fig. 9. Rate of Data Packet Successful Transmission

detection of our algorithm is 0, and the probability of successful detection is 100%.

Observing simulation results, our detection algorithm detects all collision attack, exhaustion attack and unfairness attack successfully when intrusion happen. At the same time, we don't make any fault alarm when no intrusion existed. Furthermore, our defense algorithm schedule protection plan successfully. According to figure 5,7 and 9, rate of success transmission increases about 10%. According to figure 6,8 and 10, the average energy consumption decreases about 5% per packet. According to Table 2, the first die time is prolonged around 100%.

V. CONCLUSIONS

In this paper, we studied the security on MAC layer of WSN, and applied intrusion detection and defense into original RTS/CTS-based MAC protocol. Our algorithm can decrease the attack and energy waste to some degree. Furthermore, this algorithm doesn't require any additional hardware or

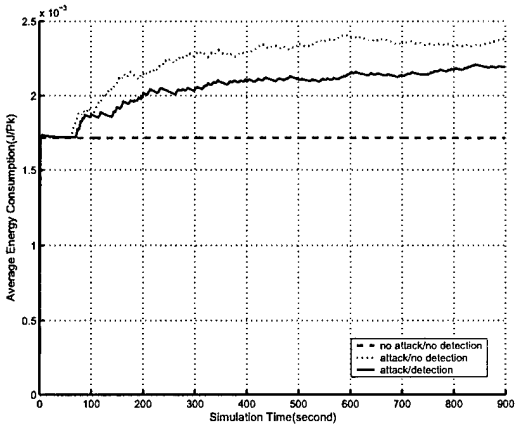


Fig. 10. Average Energy Consumption

cooperation among nodes. Simulation results show that our protocol for WSN works very well.

ACKNOWLEDGEMENT

This work was supported by the U.S. Office of Naval Research (ONR) Young Investigator Program Award under Grant N00014-03-1-0466.

The authors would like to thank Ms. Haining Shu for reviewing the whole paper and providing some comments, most of which we have cooperated into the final version.

REFERENCES

[1] A. D. Wood, J. A. Stankovic, " Denial of service in sensor networks ," *IEEE JNL* , Vol 35, Issue 10, Oct. 2002 pp54-62

[2] A. D. Wood, J. A. Stankovic, " Defeating distributed denial of service attacks ," *IEEE JNL* , Vol 2, Issue 4, July-Aug. 2000 pp36-42

[3] V. Rajaravivarma, Y. Yang, T. Yang, " An overview of Wireless Sensor Network and applications ," *Proceedings of the 35th Southeastern Symposium*, March 2003 pp432-436

[4] C. K. Toh, " Ad Hoc Mobile Wireless Networks: Protocols and Systems ," ISBN 0-13-007817-4

[5] H. Chan, A. Perrig, " Security and Privacy in Sensor Networks ," Security Oct. 2003, pp.103-105

[6] M. K. Chirumanilla, B. Ramamurthy, " Agent Based Intrusion Detection and Response System for Wireless LANs ," *ICC '03. IEEE International Conference on* , Vo. 1 , 2003, pp.492 - 496

[7] J. E. Dickerson, J. Juslin, O. Koukousoula, J. A. Dickers, " Fuzzy Intrusion Detection ," *Joint 9th IFSA World Congress and 20th NAFIPS International Conference*, Vo. 4, 2001, pp.2165-2170

[8] O. Kachirski, R. Guha, " Effective Intrusion Detectin Using Multiple Sensors in Wireless Ad Hoc Networks ," *SIGCOMM'03*, Aug. 2003

[9] " 802.11 Standard ," *http://grouper.ieee.org/groups/802/11*

[10] A. Perrig, R. Szewczyk, J. D. Tygar, D. Culler, " SPINS: Security Protocols for Sensor Networks ," Wireless Networks 8, pp.521-534, 2002

[11] J. M. Mendel, " Uncertain Rule-Based Fuzzy Logic Systems: Introduction and New Directions ," ISBN: 0-13-040969-3

[12] W. B. Heinzelman, A. P. Chandrakasan, H. Balakrishnan, " An Application-Specific Protocol Architecture for Wireless Microsensor Networks ," *IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS*, Vol. 1, NO.4, OCT. 2002

[13] E. H. Mamdani, " Applications of fuzzy logic to approximate reasoning using linguistic systems", *IEEE Trans. on Systems, Man, and Cybernetics*, vol. 26, no. 12, pp. 1182-1191, 1977.

[14] J. M. Mendel, "Fuzzy Logic Systems for Engineering : A Tutorial," *Proceedings of the IEEE*, vol. 83, no. 3, pp. 345-377, March 1995.

[15] J. M. Mendel, *Fuzzy logic systems for engineering: A tutorial*, Proc. IEEE, vol. 83, pp. 345-377, Mar. 1995